JIU/REP/2021/3

United Nations

Cybersecurity in the United Nations system organizations

Report of the Joint Inspection Unit

Prepared by Jorge Flores Callejas, Aicha Afifi and Nikolay Lozinskiy

JIU/REP/2021/3

Cybersecurity in the United Nations system organizations

Report of the Joint Inspection Unit

Prepared by Jorge Flores Callejas, Aicha Afifi and Nikolay Lozinskiy

United Nations • Geneva, 2021

Project team:

Jorge Flores Callejas, Aicha Afifi, Nikolay Lozinskiy, Inspectors

Vincent Hermie, Evaluation and Inspection Officer

Szilvia Petkov, Associate Evaluation and Inspection Officer

Hervé Baudat, Research Assistant

Dejan Dincic, Consultant

Charlotte Claveau, Alina Datsii, Bianca Canevari, Interns

Executive summary

Cybersecurity in the United Nations system organizations

In today's digitalized world, cybersecurity has emerged as a matter of importance for international organizations, and the United Nations is no exception. The digital transformation, the increasing dependence on information and communications technology (ICT) and cyberenabled solutions, and the fact that cyberthreats are constantly growing, both in sophistication and in disruptive potential, have led to an unprecedented augmentation of cybersecurity risks facing the United Nations system. Even though cybersecurity first emerged in the sphere of ICT, now that information management systems are deeply ingrained in most business activities, and the threat landscape has evolved considerably, requiring more than mere technology-driven defences, it no longer seems viable to view cybersecurity through the restrictive lens of ICT alone. In the present report, the Inspectors make an argument for integrating cybersecurity considerations into broader organizational frameworks such as enterprise risk management, business continuity planning, and safety and security, and for mainstreaming the issue across the entire organization.

In recent years, there has been a growing understanding in the United Nations system that cybersecurity requires attention. The potential consequences of a weak cybersecurity posture indeed go beyond the disruption of ICT infrastructure and systems or the volume of data that ends up compromised. Rather, the ability of the United Nations system organizations to deliver their mandates, and their credibility vis-à-vis their members and beneficiaries, is at stake. Moreover, many categories of individuals whose data the United Nations system organizations hold may be exposed to significant adverse consequences in the event of leakage. While cyberattacks may affect organizations with diverse mandates and structures differently, the menace is a real and shared one. No organization can expect never to experience a cybersecurity incident, regardless of how prepared or vigilant it is. Moreover, the reputational, operational, legal and financial implications can be considerable if the risks are neglected.

Objectives of the present review and structure of the report

The main objectives of the present review are: (a) to identify and analyse common cybersecurity challenges and risks faced by United Nations system organizations individually, as well as their respective response thereto, bearing in mind organizations' context-specific requirements (vertical perspective); and (b) to examine current inter-agency dynamics facilitating a system-wide approach to cybersecurity for better coordination, collaboration and information-sharing among the United Nations system organizations, and, where appropriate, the potential for shared solutions (horizontal perspective).

Building on the self-assessment provided by the participating organizations, the Inspectors first present a snapshot in chapter II of the cybersecurity landscape facing the United Nations system, describing the most prevalent types of threats and means of attack, with indications of their reported impact, and drawing attention to select technical issues for further consideration. In chapter III, the Inspectors examine the institutional arrangements and related practices in the United Nations system organizations in reference to a set of key elements identified in the course of the review that contribute to organizational cyberresilience and highlight good practices where applicable. In chapter IV, the focus is on the inter-agency machinery aimed at fostering coordination and collaboration among the United Nations system organizations and the operational capacities permitting the development and implementation of shared cybersecurity solutions, where such solutions make sense. There is a consensus among experts that the response must be grounded in each organization's own characteristics and requirements (based on its mandate, the information owned or managed, exposure, resources, etc.). At the same time, the United Nations system organizations do not operate in isolation and are

interconnected in many respects, including through joint programming and a degree of interdependency in their mandates and activities. It is therefore crucial to recognize areas of common exposure as well as to explore areas amenable to a concerted approach.

Cybersecurity in the United Nations system

Not a single United Nations system organization can claim not to have experienced some form of cyberattack, whether large or small. Malicious actions targeting either users of information systems (through phishing, identity theft, "man in the middle" schemes, etc.) or infrastructure (malware, distributed denial of service attacks, etc.) are by far the most prevalent source of threats reported. While cybersecurity threats are commonly associated with sophisticated technical operations, the expert community sees a discernible shift from hackers attacking servers, networks and end point devices to hacking people, using social engineering techniques aimed at manipulating individuals into divulging sensitive information for fraudulent and other illicit purposes. The coronavirus disease (COVID-19) pandemic further exacerbated the risks related to social engineering: more than two thirds of the participating organizations reported a sharp increase in cybersecurity threats and vulnerabilities during the global lockdowns that disconnected many users from centrally managed cybersecurity resources.

At the same time, the reported impact of the incidents experienced by the participating organizations was limited, which might lead to a premature conclusion that there is no serious cause for concern. This is not the conclusion the Inspectors have drawn. First, the data collected necessarily imply some blind spots, including those resulting from an understandable reluctance to expose the known level of vulnerability and from the opaque nature of cyberactivities more generally, suggesting that the exact magnitude of the threat and related consequences may simply be unknown. Most of the time, especially in the case of more sophisticated attacks, adversaries have no incentive to reveal their presence nor the vulnerabilities they have exploited, which suggests that the number of system breaches and data leaks is likely to be significantly higher than what is reported. The proportion of "known unknowns" compared with what is known about the magnitude of the cybersecurity threat is large, but the share of "unknown unknowns" may be of even greater concern. Therefore, judging the seriousness of the threat by the extent to which it is known to have materialized in the past would be misguided. The potential for damage remains high and requires sustained attention and prioritization.

Difference in the maturity of organizations and select aspects of technological preparedness

The present review was not intended to provide a comprehensive assessment of the robustness of the operational arrangements or the technical infrastructure of each participating organization, but rather to gain an understanding of the general capacities in place and isolate some common issues that may deserve special attention. For obvious reasons associated with the subject of the present review, the Inspectors chose not to reveal specific organizational arrangements that could jeopardize the security of the entities concerned. Keeping in mind the limitations inherent in information gathered primarily through self-assessment, as well as the considerable variation in the level of detail provided by the respondents, the Joint Inspection Unit (JIU) observed significant differences in the approach the participating organizations have taken in their respective responses to cybersecurity threats and, as a consequence, in the maturity of their cybersecurity posture. These differences can be explained by reference to: the setting in which each organization operates; the requirements dictated by the type of data held; the level of understanding and the priority accorded to cybersecurity by their leadership; the organizations' own historical perspective; the availability of resources; and the great variety of ICT systems, tools and software solutions used across the system.

Participating organizations were of the view that they had well understood the core technical aspects of cybersecurity and had invested in it in accordance with their own respective abilities. With regard to technological and operational capacity, the Inspectors limited their analysis to highlighting a series of issues that might deserve more focused

attention, such as: end point device management and tools facilitating remote work, in particular in the context of the COVID-19 pandemic; risks associated with the remnants of legacy systems procured in the past or built in-house over time, which might no longer be supported by contemporary security scans and fixes; the continued expansion of the use of cloud computing; organizational arrangements for vulnerability management; and shadow information technology (shadow IT) practices that involved the use and implementation of technological tools outside of the corporate ICT framework. It should be noted that, despite many challenges encountered, the advent of the pandemic also prompted some positive developments. United Nations entities were pressed to take a closer look at their security management frameworks, and planned corporate ICT projects started to materialize, driven by immediate necessity. It can be said that the massive switch to remote working at very short notice led many organizations to accelerate their efforts towards improving remote access security and may have provided a much-needed impetus to galvanize action in this regard.

Elements contributing to improved cyberresilience

The Inspectors examined a series of elements likely to improve the corporate cybersecurity posture of the United Nations system organizations and their capacity to identify, prevent and detect cyberthreats, as well as to respond to and recover from incidents. A multifaceted approach is required and involves all levels of the organization: legislative and governing bodies; oversight mechanisms; executive management; mid-level managers of both administrative and substantive or business units; and the workforce at large. In addition, the cross-cutting nature of the domain necessitates a broader outlook that goes beyond ICT and firmly embeds cybersecurity in enterprise risk management, as well as striving for greater convergence between physical security and cybersecurity. Last but not least, specialized internal human resource capacity complemented with services sourced from external providers to address specific, ad hoc needs and financial resource allocation commensurate with the needs of each organization form the backbone of a sturdy cybersecurity posture. In sum, the degree to which these elements are reflected in an organization's approach to cybersecurity directly influences its cyberresilience. The Inspectors therefore recommend that the executive heads initiate an organization-wide review to study the extent to which each of these elements, as detailed further below, is integrated into organizational policies and practices, and report the results to their legislative and governing bodies with a view to receiving guidance on how to further reinforce cyberresilience, considering the strengths and weaknesses identified in that process (recommendations 1 and 2).

Legislative and governing bodies to provide strategic guidance and resources

In the United Nations system, cybersecurity is still perceived as a predominantly technical issue, which may explain why the extent to which legislative and governing bodies have been called upon, or themselves called for, engagement on the topic has been limited in most organizations to date. In the light of the broader dimensions of cybersecurity identified in the present report, the Inspectors are of the opinion that legislative and governing bodies should step up their engagement on the matter and provide high-level strategic guidance, including through the formulation of an explicit risk appetite statement and the corresponding allocation of resources to contribute to attaining the desired level of protection. More generally, executive management should reflect on the ways in which regular reporting on cybersecurity matters to the legislative and governing bodies is undertaken and used to facilitate interaction with those bodies, within the bounds of what can be considered necessary and sufficient without jeopardizing the defences of the organization. Considering the abrupt and potentially high-impact nature of cybersecurity incidents, the Inspectors also advise organizations to anticipate the need for, and the procedures to be followed in cases requiring, the escalation of incidents to the legislative and governing bodies, both internally and among the members of such bodies themselves.

Attention of oversight bodies contributes to enhanced cybersecurity measures

Internal and external oversight mechanisms in the United Nations system organizations were found to have been attentive to cybersecurity matters even in the absence of specific references in their mandates to the topic as such. The Inspectors came across several examples of corporate enhancements made to the cybersecurity framework of participating organizations that had originated in oversight recommendations (e.g. the creation of a chief information security officer position, recommendations on training, establishment of an actionable road map, etc.). Audit and oversight committees in fact address cybersecurity issues as part of their mandate covering corporate enterprise risk management rather than in the context of ICT governance. It is commendable that these committees have embraced the topic, not only to support management but also as a way of informing legislative and governing bodies about relevant cybersecurity risks, enabling them to contribute to organizational risk mitigation. To ensure that all oversight bodies add maximum value from a cybersecurity point of view, it is important that the knowledge and experience of the cybersecurity experts within an organization inform and feed into the work of the oversight function.

Regulatory frameworks, compliance and accountability

Participating organizations refer to a wide range of industry standards on cybersecurity, sometimes more than one, with most of them either having already obtained certification under ISO 27001, planning to do so, or having chosen to voluntarily align their framework with that standard without seeking formal certification. The Inspectors refrain from arguing for one industry standard or for a harmonized, system-wide approach in this regard, because different standards may validly serve different purposes and offer suitable choices for different levels of maturity. Nevertheless, there is a strong case to be made for drawing inspiration – whether formally or informally – from relevant industry standards when setting up and managing one's own regulatory framework. Participating organizations must therefore identify the adequate standard and, within that standard, the most relevant controls, based on the level of protection required to match their own situation, depending on the requirements and risks identified through a proper organization-specific cybersecurity risk assessment.

Several leading industry standards require the existence of specific cybersecurity policies and documented procedures as a key pillar of the controls that underpin an entity's approach to cybersecurity. With few exceptions, participating organizations can be said to have recognized the importance of having an articulated reference framework in place to guide their approach to cybersecurity. High-level ICT strategies generally include cybersecurity considerations, albeit to varying degrees of elaboration. More than two thirds of the participating organizations have developed instruments specifically on cybersecurity, with three of them currently revising their framework and four being in the process of developing dedicated policies. At the same time, in four participating organizations the cybersecurity function, including the associated regulatory framework, was considered to be nascent at most. The question of compliance – and particularly enforcement in the event of non-compliance – with the guidance in place inspired less confidence in the existence of a corporate cybersecurity culture across the system. In the Inspectors' view, this warrants a closer look and more nuanced approaches to enhance accountability for breaches and to protect the organizations more generally.

Cybersecurity culture cascades from the leadership down

The first step towards instilling a culture of cybersecurity is for senior leadership itself to be aware of the associated risks and develop an understanding of the implications of poor cyberhygiene. This entails a more active stance on the part of senior managers in ensuring that internal governance mechanisms are set up in a way that supplies them with the information and evidence base they need. The role of executive management in this regard goes beyond its decision-making on the allocation of resources. A key element is to encourage an internal culture in which acknowledging and proactively keeping track of the

occurrence of incidents is not seen as an admission of failure but rather as a starting point for jointly addressing a shared problem and for better protecting the organization and its assets. Additional ways in which executive management can inspire action and influence mindsets down the chain of command in concrete terms are by modelling recommended behaviours, ensuring managerial accountability across the organization, participating in awareness-raising programmes and displaying an engaged leadership style on cybersecurity matters overall. A cultural shift is needed in the United Nations system, and the contribution of executive managers in setting the tone from the top is essential to achieving it.

Mainstreaming cybersecurity as a whole-of-organization endeavour

In line with the growing understanding that responsibility for cybersecurity cannot rest with ICT departments alone, the majority of participating organizations have recognized, in one way or another, that administrative as well as substantive departments have a role to play. However, the information gathered during the present review suggests that organizational units across the board may still not be sufficiently receptive to including cybersecurity and resilience requirements in the design and implementation of their projects and activities. In some quarters, cybersecurity policies and procedures were said to be viewed as an impediment to operational agility and efficiency rather than as protective shields for the reputation and assets of the organizations. It is particularly important that executive heads actively counteract such perceptions. Rendering the cybersecurity dimensions of programmatic and administrative functions more explicit can reduce misunderstandings regarding the complementary roles and responsibilities of different departments and can address the lack of ownership detected among some stakeholders during the present review. The mainstreaming of cybersecurity considerations in the policies and practices governing the work of all departments would in itself be an acknowledgement that each function in an organization has a contribution to make towards achieving a whole-of-organization approach to the matter.

The workforce as a first line of defence

The challenge of educating every member of the workforce on his or her role in protecting the information and digital assets of the organization, as well as the importance of adhering to cybersecurity policies, procedures and best practices, persists. The human factor has gained in importance not only in the overall cybersecurity threat landscape, as reflected in the global concern over individual end users being increasingly targeted, but also as an important element in the defence structure of the participating organizations, provided that such users are properly educated. The realization that the responsibility for cyberprotection starts with well-informed and vigilant users has triggered significant efforts in terms of training and awareness-raising initiatives, despite resource limitations, users' training fatigue and the difficulties in keeping up with the constant evolution of the subject matter. Nonetheless, the multitude of programmes and individual initiatives did not appear to be pursued in a consistent, systematic or risk-based manner. The Inspectors therefore advise organizations to aim for developing a comprehensive training and awareness-raising programme designed as a proactive tool for changing the internal culture through the establishment of clear objectives defined for each category of stakeholder depending on the risks they may represent for the organization, rather than offering individual modules to everyone without being guided by a strategic vision. Paying attention to occasional users of corporate ICT systems, including conference delegates, interns, visitors and other non-staff categories of personnel, is crucial, since such users are often logging on to corporate infrastructure with personal devices. Moreover, being infrequent users of the systems in question, they are less likely to be conversant in their correct and safe use in accordance with applicable organizational policies and practices.

Optimization of cybersecurity expenditure and investment

Estimating the resources currently dedicated to cybersecurity represents a challenge, due to the characteristics of the financial and budgetary frameworks of the United Nations

system organizations and their practices in managing and accounting for such resources. It goes without saying that a well-protected cybersecurity framework comes at a price. Despite the reported increase in resources allocated to cybersecurity, practitioners in the United Nations system still perceive resource shortages as an obstacle to enabling their organizations to cover all aspects of cyberresilience. An important point to bear in mind is that the amount spent on cybersecurity does not automatically reflect the level of protection. More than debating how much, the key is to determine where the resources should be allocated so as to have the most meaningful impact. Irrespective of the amount of funding available, the information gathered does not point to a consistent approach to the prioritization of cybersecurity spending by the United Nations system organizations, thereby increasing the risk of an inefficient use of already scarce resources. To optimize cybersecurity expenditures, as well as related investments, a thorough cyberrisk assessment culminating in a business case detailing costs, benefits, risks and expected savings, as well as referencing the potential financial implications of not making the investment, is a prerequisite for enlisting the support of and obtaining an adequate level of resource allocation by legislative and governing bodies.

Internal expert capacity for cybersecurity

More than half of the participating organizations have built specialized and dedicated human resource capacity in-house, ranging from a single information security expert, sometimes assigned only part-time, to a larger organizational unit headed by a chief information security officer. In contrast, in 10 participating organizations cybersecurity tasks are handled mainly by ICT officers alongside their other duties. In the cybersecurity domain, there is a high incidence of using external expertise due to its complex technical nature, which is evolving constantly and requires a considerable degree of specialization that is challenging and costly to keep available and current on a permanent basis. Resorting to external providers to boost and complement internal capacity is unavoidable and even desirable, so as to stay responsive to fast-paced developments in cyberspace. The degree to which this is done lies within the discretion of each organization, based on its own needs and context. However, in the Inspectors' view, it is important for organizations to retain an appropriate degree of control, oversight and technical capability internally to effectively manage and interface with the capacities contributed by external providers. Being able to rely on a dedicated chief information security officer function in this regard can provide the focus and assurance needed for this purpose. The core functions falling under the responsibility of the chief information security officer go beyond the elaboration of controls at the operational level and by default include a managerial dimension to ensure the fullest possible reflection of cybersecurity considerations as a matter of organizational risk and resilience management.

Noting the disparities in the internal set-up observed across the participating organizations, which may be more indicative of the constraints faced rather than a deliberate or strategic choice, the Inspectors believe that having dedicated and specialized cybersecurity expertise available in-house contributes to reinforcing the posture of the organization but also of the system as a whole and is a worthwhile investment to consider. In addition, it would be prudent for each organization to assess whether it may benefit from pursuing the establishment of a security operations centre, even in the most rudimentary form, which should be based on an organization-specific cost-benefit analysis involving parameters such as the complexity of the organization's ICT infrastructure set-up, the number and type of critical assets and processes managed, the overall volume of data flows and hence the threat frequency, and other factors. One of the important aspects of a formal security operations centre, regardless of its size and capacity, is the focus it provides for monitoring operations on a daily basis and for performing a crucial coordination and synchronization role, as well as raising organizational awareness, which can make a significant difference with regard to an efficient allocation of internal resources and capacities.

Cybersecurity – a system-wide priority?

Strengthening the cybersecurity posture of the United Nations system through

deeper coordination and collaboration among organizations at the strategic level and through an enhanced system-wide operational capacity has been stated over the years as a priority, both by Member States and by executive management. However, despite the existence of several important resources, mechanisms and initiatives available within the system, including apparent political will, progress in making these aspirational statements a reality has been less than evident. To date, there is no single entity formally tasked with driving the agenda of a harmonized approach to cybersecurity, with system-wide efforts on cybersecurity being concentrated institutionally around inter-agency coordination mechanisms under the United Nations System Chief Executives Board for Coordination, and operationally supported, to a degree, by the United Nations International Computing Centre as a provider of shared cybersecurity services for several United Nations system organizations. In the present review, the Inspectors found that there were insufficient linkages between system-wide strategic direction and operational capacity, which had affected the dynamic between those structures and was likely to be costing the system dearly in terms of unrealized efficiency gains due to missed opportunities for more direct collaboration.

Basic level of protection and agreed minimum defence requirements needed

The idea that weak protection against cyberthreats in one organization makes the whole system more vulnerable is generally accepted. It can thus be said that the United Nations system is as strong as its weakest link. However, past initiatives aimed at introducing common benchmarks or comparative maturity assessments across organizations received insufficient support, with detractors citing the diversity of the structural set-ups and the context in which the organizations operated as an obstacle limiting the value of such collective or cumulative approaches. Moreover, participating organizations displayed little appetite at senior levels for sharing their internal cybersecurity information, for reasons of confidentiality and concerns about the exposure of vulnerabilities even among the organizations. These concerns could be mitigated by way of information-sharing agreements, which could provide for appropriate safeguards. However, attempts to institute system-wide operational capacity for preventing, detecting and responding to cyberthreats have yet to yield tangible results. Some of the gaps in this regard have been filled by the United Nations International Computing Centre, whose portfolio of cybersecurity services has attracted a sizeable client base, albeit on an opt-in basis, thereby catering to the needs of the system only partially. Despite the limited success to date of system-wide endeavours towards a common or concerted approach, whether at a conceptual or operational level, the Inspectors believe that determining a basic level of protection and minimum defence requirements for the United Nations organizations, and therefore for the system as a whole, remains a valid objective that continues to be worth pursuing.

Inter-agency mechanisms on cybersecurity

The inter-agency machinery dealing with cybersecurity was found to be long established and generally functioning, even though some of the ambitious goals it had set for itself had yet to be translated into tangible outcomes beyond the solid level of information-sharing and system-wide professional exchange it had already enabled. The records of the Digital and Technology Network and the High-level Committee on Management provide evidence of the fact that, over a period of at least 30 years, cybersecurity has featured with some prominence on the system-wide agenda. Since 2011, the Information Security Special Interest Group, which operates under the Digital and Technology Network, has been the principal mechanism for promoting inter-agency cooperation and collaboration to optimize information security within its member organizations. According to its terms of reference, its main purpose is that of knowledge-sharing, yet, following the revision of those terms of reference in 2018, emphasis is also placed on its role in undertaking joint projects – an aspiration that was further amplified by its parent Network's call for the Information Security Special Interest Group to become more active in the design and delivery of shared solutions and innovation. Acknowledging the professional credibility and considerable body of work produced by the group over the

years, the Inspectors found that large-scale shared solutions for the system had not been realized as mandated. As a coordination body, the Information Security Special Interest Group faces the same challenges in this regard as any other inter-agency mechanism in the absence of decision-making authority to compel action directly at the system level, which is why it would be unrealistic to expect implementation to materialize within that forum. The impact of the Information Security Special Interest Group is somewhat limited by its reliance on the individual engagement and follow-through of the organizations it brings together, by the uneven empowerment of its members within their own institutional architecture and by the fact that the Group has no operational capacity to implement agreements reached or recommendations made. In addition, the Group reports to the Digital and Technology Network, thereby mirroring the prevailing set-up observed within most organizations whereby the chief information security officer reports to the head of his or her respective ICT department, with all the benefits and limitations that such a set-up implies.

United Nations International Computing Centre as a key cybersecurity service provider for the system

The United Nations International Computing Centre has been providing cybersecurity services to about two thirds of the United Nations system organizations for a number of years, although the client base for each of its 13 related services varies greatly. This area of its service catalogue has seen considerable and diverse growth, even though it still represents only a fraction of the Centre's business in budgetary terms. The assessment of the United Nations International Computing Centre cybersecurity services was found to be uneven among the participating organizations, with the Common Secure Threat Intelligence service recognized as its flagship service. Already in 2019, JIU advocated for better leveraging of the unrealized potential of the Centre, specifically concerning its services in the area of cybersecurity. United Nations system organizations and the Centre are encouraged to find more common ground to complement existing internal capacities of the organizations with more shared services. In that spirit, the executive heads of the participating organizations are invited to reconsider current corporate arrangements and revisit opportunities for utilizing the Centre's cybersecurity services. As an inter-agency facility that operates under the rules and administrative framework of the World Health Organization, the United Nations International Computing Centre's business model is based on a cost-recovery and shared service model. This combination has proven to be both an enabler and an obstacle for the Centre to become a cybersecurity hub for the system. It has created a situation in which the United Nations International Computing Centre's service offer is dependent on clients providing seed funding to upfront the costs of developing a new service to meet demand, while many can only afford to buy the service so developed once a critical mass of clients has already subscribed to it. Considering the challenges imposed by cybersecurity and the risks faced by the organizations, it was considered timely to explore the use of voluntary contributions as a complementary funding mechanism to provide more direct resources for safeguarding the overall cybersecurity posture of the system. The Inspectors consider that the establishment of a trust fund to complement existing funding mechanisms with voluntary contributions earmarked for shared cybersecurity solutions benefiting the system has the potential to become a game changer in addressing some of the stumbling blocks in this regard. The trust fund would not only allow Member States wishing to contribute directly to cybersecurity enhancements across the system to do so but would also provide an opportunity, through a governance mechanism for the fund to be devised by the relevant stakeholders, to improve linkages between the strategic direction that the Information Security Special Interest Group can provide and the operational capacity offered by the United Nations International Computing Centre (recommendation 3). The General Assembly is invited to take note of the recommendation and to invite donor contributions to the trust fund (recommendation 4).

Towards a closer alignment of physical security and cybersecurity considerations

It is well known that the Department of Safety and Security has a system-wide mandate to set policy and guide operational arrangements in the sphere of physical safety and security across entities globally. Despite the convergence between the physical space and cyberspace when it comes to protecting personnel and organizational assets, the Department of Safety and Security's mandate as given by the General Assembly focuses on specific safety and security threats falling within its purview and thus does not contain any explicit reference to cybersecurity or the cyberdimension of the risks and threats. The need for a closer alignment between physical security and cybersecurity has evidently inspired debate in several inter-agency bodies for years, but this has yet to mature into actionable conclusions for the system. To help clarify the opportunities and risks associated with extending to the cyberrealm the prevailing risk-based approach and the structured, accountability-centred response that underpins the United Nations Security Management System, the Inspectors recommend that the Secretary-General present a report to the General Assembly, which should highlight how a more holistic protection of United Nations personnel and assets can be leveraged and should indicate necessary measures to strengthen the existing structures accordingly, giving particular attention to the role of the Department of Safety and Security in this regard. The report should be informed by the outcomes of consultations between relevant inter-agency coordination mechanisms that deal with cybersecurity and the Inter-agency Security Management Network, with input from the United Nations International Computing Centre as appropriate (recommendation 5).

Recommendations

Recommendation 1

The executive heads of the United Nations system organizations should prepare, as a matter of priority and no later than 2022, a comprehensive report on their cybersecurity framework and present it to their respective legislative and governing bodies at the earliest opportunity, covering the elements contributing to improved cyberresilience examined in the present report.

Recommendation 2

The legislative and governing bodies of the United Nations system organizations should consider the reports on the elements contributing to improved cyberresilience prepared by the executive heads and provide strategic guidance on further improvements to be implemented in their respective organizations, as necessary.

Recommendation 3

The Director of the United Nations International Computing Centre should seek to establish by no later than the end of 2022 a trust fund for donor contributions, which would complement the capacity of the Centre to design, develop and offer shared services and solutions to enhance the cybersecurity posture of the United Nations system organizations.

Recommendation 4

The General Assembly of the United Nations should, no later than at its seventy-seventh session, take note of the recommendation addressed to the Director of the United Nations International Computing Centre to establish a trust fund for shared cybersecurity solutions and invite Member States wishing to reinforce the cybersecurity posture of the United Nations system organizations to contribute to the trust fund.

Recommendation 5

The Secretary-General should present a report to the General Assembly of the United Nations no later than at its seventy-eighth session exploring further opportunities to draw upon the convergence between physical security and cybersecurity so as to ensure a more holistic protection of United Nations personnel and assets and indicating necessary measures to strengthen the existing structures accordingly, giving particular attention to the potential role of the Department of Safety and Security in this regard.

These formal recommendations are complemented by 35 informal or soft recommendations indicated in bold text in the body of the present report, as additional suggestions that, in the view of the Inspectors, could enhance the cybersecurity posture of the United Nations system.

Contents

Acronyms and abbreviations

CEB	United Nations System Chief Executives Board for Coordination
FAO	Food and Agriculture Organization of the United Nations
IAEA	International Atomic Energy Agency
ICAO	International Civil Aviation Organization
ICT	information and communications technology
ILO	International Labour Organization
IMO	International Maritime Organization
ISO	International Organization for Standardization
ITC	International Trade Centre
ITU	International Telecommunication Union
JIU	Joint Inspection Unit
NGO	non-governmental organization
Shadow IT	shadow information technology
UNAIDS	Joint United Nations Programme on HIV/AIDS
UNCTAD	United Nations Conference on Trade and Development
UNDP	United Nations Development Programme
UNEP	United Nations Environment Programme
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNFPA	United Nations Population Fund
UN-Habitat	United Nations Human Settlements Programme
UNHCR	Office of the United Nations High Commissioner for Refugees
UNICEF	United Nations Children's Fund
UNIDO	United Nations Industrial Development Organization
UNODC	United Nations Office on Drugs and Crime
UNOPS	United Nations Office for Project Services
UNRWA	United Nations Relief and Works Agency for Palestine Refugees in the Near East
UN-Women	United Nations Entity for Gender Equality and the Empowerment of Women
UNWTO	World Tourism Organization
UPU	Universal Postal Union
WFP	World Food Programme
WHO	World Health Organization
WIPO	World Intellectual Property Organization
WMO	World Meteorological Organization

I. Introduction

A. Context

1. **Importance of cybersecurity in the digital age.** In today's digitalized world, cybersecurity has emerged as a matter of importance for international organizations, and the United Nations system organizations are no exception. The digital transformation, the increasing dependence on information and communications technology (ICT) and cyberenabled solutions, and the fact that cybersecurity threats are constantly growing, both in sophistication and in disruptive potential, have led to an unprecedented augmentation of cybersecurity risks facing United Nations system organizations. Incidents that would once have been considered extraordinary are becoming more frequent and commonplace. The Inspectors recall a letter addressed to the Secretary-General in 2017, in which the representatives of the United Nations system oversight committees, on the occasion of their first ever joint meeting, identified among the three core concerns for the United Nations system organizations the need for management to give due consideration to new and emerging risks, in particular the global and business critical threats posed to cybersecurity, and the risks emerging from new ways of working as digital transformation gathered pace.[1] Against this backdrop, the participating organizations of the Joint Inspection Unit (JIU) supported an examination by the Unit of the cybersecurity policies and practices in place in the United Nations system, which was conducted by JIU as part of its programme of work for 2020 and represents the latest in a series of technology-themed reviews on topics such as ICT governance, Internet website management and the use of cloud computing services.[2]

2. **United Nations system as a target of cyberattacks.** The cybersecurity threat landscape facing United Nations system organizations is no different from those affecting other entities, in that the instigators, means and objectives of the attacks – ranging from financial to symbolic – are the same. A distinction, if any, may be detected in the ways in which the United Nations may be considered a preferred target compared to other private and public sector entities. For one, the appeal may lie in the United Nations entities' high visibility and global scope, which makes them a more prominent target for hackers in search of fame, in comparison with the publicity to be gained by attacking any one national government or public sector entity. In addition, in contrast to many private sector targets, they may also be more attractive for "hacktivists" who are guided by ideological motives and protest or oppose values that United Nations system organizations stand for or propagate. Due to the intergovernmental setting in which the organizations operate, there is also an undeniable political dimension, which is only hinted at by the organizations themselves but, without exception, acknowledged as a given. In sum, while the methods of attack are identical, the motives may differ. What is clear is that there has been an exponential increase in attacks, large and small, against JIU participating organizations over the last five years, as evidenced by figures consulted by the Inspectors from various sources.

3. **Cybersecurity incidents go beyond system disruption and may affect mandate delivery.** For the United Nations system organizations, the potential consequences of a weak cybersecurity posture go beyond the disruption of administrative processing capacity and ICT infrastructure and systems and should not be measured solely by reference to the volume of information and data that end up compromised. A single breach can be devastating for the organization if it impacts sensitive data such as personally identifiable information, staff medical records, intellectual property data, historical and political archives or similar. Moreover, organizations' ability to deliver their mandates, as well as their credibility vis-à-vis their member States and beneficiaries, is at stake. In the sphere where these organizations

[1] Letter addressed to the Secretary-General, 26 January 2017.

[2] JIU/REP/2008/5; JIU/REP/2008/6; JIU/REP/2011/9 and JIU/REP/2019/5.

operate, even technologically minor incidents can produce ripple effects that might interfere with diplomatic and intergovernmental processes, humanitarian interventions, or, in the worst case, even international peace and security. While cyberattacks may affect United Nations system organizations with diverse mandates and structures differently, the threat is a real and shared one.[3] No organization can expect never to experience a cybersecurity incident, regardless of the level of its preparedness and vigilance. However, the reputational, operational, legal and financial implications could be considerable if the risks are neglected.

4. **Recognition of the importance of cybersecurity by the international community and the United Nations.** The understanding that hostile activities in cyberspace pose a threat both to the international community and to the United Nations organizations more specifically has been documented in the resolutions and reports of relevant legislative and governing bodies and internal coordination mechanisms since at least the early 1990s. Substantive debate on the issue has been pursued on parallel tracks. On the one hand, it is pursued among Governments as members of United Nations legislative and governing bodies developing the global response to the emergence of cybercriminality and cyberthreats (the "outward-facing" dimension of the work of the United Nations on cybersecurity, for which system-wide coordination competence lies with the United Nations System Chief Executives Board for Coordination (CEB) High-level Committee on Programmes), and, on the other hand, it is pursued among United Nations system organizations looking to strengthen their internal corporate preparedness and response to related challenges, both collectively and individually (the "inward-facing" dimension, falling within the purview of the High-level Committee on Management). Recognition of the dual role of the United Nations system in this regard is evidenced by a concluding statement made by the Secretary-General in the context of CEB as recently as 2019, stating the "need for the United Nations system to take a leadership role and develop a unified position on cybersecurity and related threats, while serving as a convening platform for Member States and other stakeholders to discuss cybersecurity in its various dimensions."[4]

5. **States' responsibility to protect United Nations assets includes digital assets in cyberspace.** Insofar as legal protections in relation to cybersecurity are concerned, United Nations system organizations rely on the privileges and immunities that apply to their properties, assets, archives, documents and communication more broadly.[5] The existence of such privileges and immunities places States parties under the obligation to be in a position under their respective laws to provide the protection and security necessary for the fulfilment of the purposes of the entity that holds such privileges and immunities, and to ensure, in particular, the inviolability of premises, archives and documents, "wherever located and by whomsoever held". In other words, States, and in particular host countries, have a duty to protect organizations from hostile attacks, whether in the physical or in the digital sphere. This interpretation was confirmed to the Inspectors by the Office of Legal Affairs and settles the question of whether electronic data and digital assets are covered by existing legal provisions. In fact, in more recent headquarters and host country agreements concluded bilaterally between the organizations and the States hosting them in their territory, the Office of Legal Affairs indicated that the term "archives" had been expressly defined as including emails and computer records, as well as any such similar materials belonging to or held by the organization concerned in furtherance of its function. Protected communication has similarly been considered to include electronic data communications, whereas other agreements have more widely provided for the inviolability of whatever the means of the communications employed.

[3] For background information on the challenges faced by the United Nations system organizations, see the United Nations Digital Blue Helmets brochure produced by the United Nations Office of Information and Communications Technology.

[4] CEB/2019/2, para. 39.

[5] Article 105 of the Charter of the United Nations; the Convention on the Privileges and Immunities of the United Nations of 13 February 1946; the Convention on the Privileges and Immunities of the Specialized Agencies of 21 November 1947; and the Agreement on the Privileges and Immunities of the International Atomic Energy Agency of 17 August 1959.

In the broadest sense, this means that States have a responsibility under international law to protect United Nations assets, including in cyberspace.

6. **Evolution from ICT to a broader perspective.** Traditionally, cybersecurity considerations first emerged and were dealt with in the sphere of ICT, which, in the early days of computing, occupied a less prominent role in corporate activities than it does today. This ICT-focused understanding of cybersecurity as a discipline was the logical product of a time when threats were mostly limited to the computing infrastructure and affected a much narrower set of information assets and business processes. However, now that ICT is deeply ingrained in most business activities, and the threat landscape has evolved considerably beyond mere technical disruptions requiring simpler fixes and technology-driven defences, it no longer seems viable to view cybersecurity through the restrictive lens of ICT alone. **In fact, the Inspectors consider that cybersecurity should be framed by a much wider outlook involving several organizational domains and competences, including enterprise risk management, physical safety and security, data protection and privacy, legal expertise, and information security in the broader context of information and knowledge management.**

7. **Business continuity planning as the key to a risk-based approach to cybersecurity.** Some organizations have already started to embrace the concept of organizational resilience management encompassing cybersecurity as one aspect among many. The central preoccupation of this domain of organizational resilience is to adequately assess cyberrisks with a view to adopting preventive, risk mitigating measures and defending against threats on the one hand, and introducing adequate protocols to guide action and preserve business continuity in the event that such risks and threats do materialize on the other hand. Risk mitigation in the area of cybersecurity is never absolute, but rather a matter of degree, and its effectiveness must be judged not solely by its success in averting threats, but also by the extent to which it can help restore operations after a successful attack. When serious incidents happen, it is therefore essential to have a well-tested disaster recovery procedure for all information systems in place. This can only be achieved if recovery protocols are tested regularly and rigorously as part of routine business continuity planning, ideally employing penetration testing as a powerful risk management tool. While disaster recovery procedures have a strong technical dimension, they should be developed within the strategic parameters set by the organization's leadership (including risk tolerance and appetite, available resources, etc.) and established operational constraints (such as acceptable recovery time) in order to be effective. Accordingly, business continuity planning, alongside risk management, becomes an indispensable pillar of organizational resilience in the face of physical threats and cyberthreats alike.[6]

B. Objectives, scope and methodology

Objectives

8. The main objectives in conducting the present review are:

(a) To identify and analyse common cybersecurity challenges and risks faced by United Nations system organizations and their respective response thereto, bearing in mind relevant commonalities and differences in organizations' context-specific requirements and the capacity to protect their key assets while maintaining their ability to deliver on their mandates; and

(b) To map current inter-agency arrangements and examine whether they are effective in facilitating a system-wide approach to cybersecurity, as well as to identify opportunities for better coordination, collaboration and information-sharing among the United Nations system organizations, where appropriate.

[6] The JIU programme of work for 2021 includes a review specifically on business continuity.

Scope

9. **System-wide coverage.** The present review was undertaken on a system-wide basis and included all JIU participating organizations, namely the United Nations Secretariat, its departments and offices, the United Nations funds and programmes, other United Nations bodies and entities, the United Nations specialized agencies, and the International Atomic Energy Agency (IAEA). The International Trade Centre (ITC) did not take part in the review process and is therefore not featured in the aggregate figures included in the present report. In addition, JIU examined the United Nations International Computing Centre, considering its role in providing cybersecurity services to several organizations of the United Nations system.

10. **Focus on internal cybersecurity arrangements.** The present report focuses on corporate arrangements pertaining to the management of the cybersecurity frameworks within United Nations system organizations, which are designed to protect their assets in cyberspace and enable the delivery of their mandated activities (the "inward-facing" dimension of cybersecurity).[7] The intergovernmental work of the United Nations system in support of Member States, including through technical assistance to build national cybersecurity capacity or respond to cybercrime, is outlined in annex I for context but was not the focus of the present review. Contained in the annex is a brief historical overview of how the issue has developed under the various workstreams of the General Assembly and other intergovernmental bodies.

11. **Technical aspects not assessed in detail.** Although not purely a technological issue, cybersecurity cannot be addressed without reference to its ICT dimension. However, the Inspectors did not attempt to analyse in depth the measures implemented by the organizations with regard to their technological pertinence or soundness. For their examination of technical considerations that proved indispensable for the completeness of the present report, the Inspectors benefited from external expertise and limited themselves to highlighting select areas for consideration and potential further examination. In particular, they do not purport to provide in the present report a comprehensive assessment, comparative or otherwise, of the maturity of each organization of the United Nations system. Such an assessment was considered to be beyond the scope of the report, but also of limited utility for the organizations concerned, whether collectively or individually.

12. **Related data-centric domains of relevance to cybersecurity but out of scope.** A variety of knowledge and information management domains, as well as data protection, privacy and related domains, intersect with cybersecurity yet exceed the scope of the present study. Some have already been the subject of JIU reports (e.g. the classification of information as a subtopic of records and archives management),[8] while others are of being articulated at the level of individual organizations based on system-wide guidance (e.g. the translation of the Personal Data Protection and Privacy Principles adopted by CEB in 2018 into organizational policies and administrative issuances). In addition, the challenges and complexities associated with the introduction, in the same year, of the European General Data Protection Regulation and attempts to enforce it in relation to the United Nations system organizations presents a separate set of questions with implications for cybersecurity that exceeded the scope of the present study. Far from representing an exhaustive list, these issues illustrate the wide reach of cybersecurity as a cross-cutting domain that could be touched upon only in a cursory manner in the present report. **The Inspectors wish to note, however, that in particular the area of data protection and the privacy of personal information is an issue of significant topicality and concern, and that a dedicated critical review of United Nations system organizations' policies and practices in this regard would be timely and warranted.**

[7] The present report is complemented by a management letter addressed to the executive heads of the JIU participating organizations focusing on the risks associated with the safeguarding and protection of organizations' legal, normative, administrative, political and historical documents and data (JIU/ML/2021/1).

[8] JIU/REP/2013/2.

Methodology

13. In accordance with JIU internal standards and working procedures, the Inspectors used a range of qualitative and quantitative data-collection methods from different sources to ensure the consistency, validity and reliability of their findings. Information used in the preparation of the present report was current as at May 2021.

- **Questionnaires and desk review.** JIU gathered information through two questionnaires addressed to its participating organizations. The Inspectors examined relevant components of the applicable regulatory frameworks (governing body resolutions, corporate strategies on ICT, and specific policies and procedural guidance documents on information security and cybersecurity where they existed) and consulted reports from internal and external oversight bodies. Several rounds of queries to the United Nations International Computing Centre allowed a critical review of its mandate, service catalogue and institutional as well as operational capacity in the area of cybersecurity. The Office of Legal Affairs provided written clarification on a series of legal aspects. The analysis of the reports of the committees and networks of CEB, mainly the Digital and Technology Network and its Information Security Special Interest Group, served to provide further insight into the inter-agency dynamics and current and past system-wide initiatives. The Inspectors also consulted relevant industry standards and cybersecurity-related literature as background documentation.
- **Interviews.** Drawing on the responses to the questionnaires, the Inspectors conducted 45 interviews with officials in charge of ICT, and cybersecurity more specifically, as well as with senior officials to provide a broader organizational perspective. Subsequent interviews were conducted with representatives of oversight bodies, the Department of Safety and Security as well as select non-participating organizations. Interviews with the chair of the Information Security Special Interest Group and representatives of the CEB secretariat provided further insight into inter-agency initiatives on cybersecurity. Interviews with representatives of the United Nations International Computing Centre provided details on the cybersecurity capabilities offered by the Centre. The Inspectors also attended the 2020 Common Secure Conference, hosted by the United Nations International Computing Centre and held virtually due to the ongoing coronavirus disease (COVID-19) pandemic, to get an impression of current developments and challenges discussed among the subscribers to this United Nations International Computing Centre service. In addition, through a focus group, the Inspectors benefited from the views and experience of several chief information security officers as members of an informal worldwide network of city governments facing similar challenges, through which they learned about these city governments' policies, practices and lessons learned as a possible public sector reference for United Nations entities.

14. **Limitations in terms of availability and confidentiality of information.** The Inspectors encountered limitations primarily related to: (a) the availability of information (given that metrics on cybersecurity incidents were not systematically recorded or, when they were recorded, did not follow a commonly agreed methodology, thereby also limiting the comparability of data); (b) the confidentiality of data on threats, incidents and, in particular, response measures, as organizations were of the view that the sharing of such information created unnecessary exposure identifying and revealing vulnerabilities within their security infrastructures, which was why information was presented primarily in aggregate form in the narrative of the report, without attribution to specific entities unless warranted on a case-by-case basis; and (c) the impact of the COVID-19 pandemic on the data-collection process, resulting in delays and necessitating the conduct of interviews exclusively by video conferencing, which might have affected access to some interlocutors as well as their willingness to share sensitive information that could have otherwise been obtained through in-person interactions. In addition, although the Inspectors sought to study and reflect how participating organizations' responses to the pandemic had informed cybersecurity considerations, some arrangements and measures implemented in that context might have

evolved further and might therefore not have been fully accounted for during the review process.

15. **Acknowledgments.** The Inspectors wish to express appreciation to all the officials of the United Nations system organizations and representatives of other organizations who assisted in the preparation of the present report, particularly those who participated in the interviews and so willingly shared their knowledge and expertise. For quality assurance purposes, an internal peer review method was used to solicit comments from the JIU Inspectors on the draft report, which was subsequently circulated to the organizations concerned for substantive comments on the findings, conclusions and recommendations, as well as for the correction of any factual errors.

16. **Recommendations.** The present report contains five formal recommendations, of which one is addressed to the General Assembly, one to the legislative and governing bodies, one to the executive heads of the JIU participating organizations, one to the Secretary-General and one to the Director of the United Nations International Computing Centre. To facilitate the handling of the present report and the implementation of its recommendations and monitoring thereof, annex X contains a table indicating whether the report was submitted to the relevant organizations for action or for information and specifying whether the recommendations require action by the organizations' legislative and governing bodies or by the executive heads. The formal recommendations are complemented by 35 informal recommendations indicated in bold text, as additional suggestions that, in the view of the Inspectors, could enhance the cybersecurity posture of the United Nations system.

C. Definitions

17. **Absence of a universally accepted definition of cybersecurity.** International and national industry standards on information security often include a definition of cybersecurity. However, there is no universally accepted definition or global consensus on what the term encompasses precisely. In the United Nations context, the Inspectors noted that neither was there any system-wide guidance from the relevant inter-agency forums unanimously recommending a particular definition as authoritative for the system,[9] nor did the organizations' own regulatory frameworks systematically attempt to impose a definition of cybersecurity. In the present report, the Inspectors decided to use the definition of cybersecurity developed by the International Telecommunication Union (ITU), which is reproduced in box 1. The vast majority of JIU participating organizations confirmed that the definition was reflective of their approach to the matter, frequently complemented by their use of relevant industry standards as a reference.

[9] The United Nations-wide framework on cybersecurity and cybercrime (see CEB/2013/2) and the United Nations system internal coordination plan on cybersecurity and cybercrime (2014, annex) included definitions to establish a common understanding of the terms cybercrime and cybersecurity, with the caveat that those were functional working definitions not endorsed as such by the United Nations system.

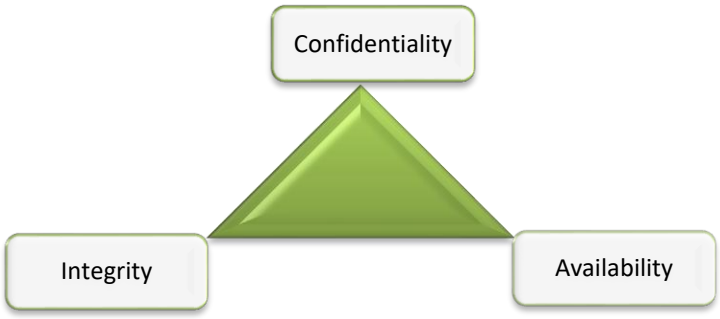
Box 1: Cybersecurity as defined by the International Telecommunication Union

"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: availability; integrity, which may include authenticity and non-repudiation; and confidentiality."

International Telecommunication Union (ITU) Recommendation ITU-T X.1205, Overview of cybersecurity.

18. **Information security versus cybersecurity.** Many organizations use the term "information security", which is concerned with the security of information in all its forms and wherever stored, not just electronic data in the digital sphere. Cybersecurity, in contrast, may be more closely associated with exclusively digital information and the protection of a broader set of assets connected to or affected by cyberspace, as seen in the ITU definition. Despite slight conceptual divergences between the two terms, they overlap to a significant extent, notably as regards the core objectives of protecting the availability, integrity and confidentiality of information (also known as the "triad of information security", as seen in figure I). Some organizations use the term "cybersecurity" fully interchangeably with the term "information security". Others consider "cybersecurity" to have replaced the more traditional term of "information security", albeit forfeiting some of its broader knowledge and information management related connotations in favour of more ICT-centric properties, and yet others employ "cybersecurity" as an umbrella term that comprises both "information security" and the narrower (and more rarely used) term "ICT security", which refers specifically to the security of ICT infrastructure (e.g. hardware, software, networks and technical processes).

Figure I
Model of the triad of information security[10]



Source: United States of America National Institute of Standards and Technology.

19. Comparable terminological ambiguities were observed in the nomenclature related to the leadership functions under which cybersecurity tended to be placed in an organizational context. For example, the "chief information security officer" may report to a "chief information technology officer" or a "chief information officer", where either the latter two are used synonymously to denote the head of the ICT department, or the chief information officer also comprises knowledge and records management or communications and public relations functions. It was not possible to discern a consistent pattern that would have suggested conceptual deliberateness or rigour in delineating differences in scope between the functions attached to each term.

20. Throughout the report, the Inspectors use the term "cybersecurity", as defined above. Whenever reference is made to "information security", it is done deliberately with the aim to be faithful to source documents in rendering direct quotes or to ensure the correct usage of technical terms, such as "chief information security officer" or "Information Security Management System". Nonetheless, the Inspectors found that there was no need to revise it or harmonize its use, as it did not represent an impediment to communicating or exchanging related information across the organizations.

[10] As defined by the Center for Internet Security, the confidentiality-integrity-availability triad is a benchmark model in information security designed to govern and evaluate how an organization handles data when they are stored, transmitted or processed. Each attribute of the triad represents a critical component of information security, as follows. Confidentiality means that data should not be accessed or read without authorization. It ensures that only authorized parties have access. Attacks against confidentiality are disclosure attacks. Integrity means that data should not be modified or compromised in anyway. The assumption is that data remain in their intended state and can only be edited by authorized parties. Attacks against integrity are alteration attacks. Availability means that data should be accessible upon legitimate request. This ensures that authorized parties have unimpeded access to data when required. Attacks against availability are destruction attacks.

II. A snapshot of cybersecurity in the United Nations system

A. Growing attention to cybersecurity, yet different maturity levels across the system

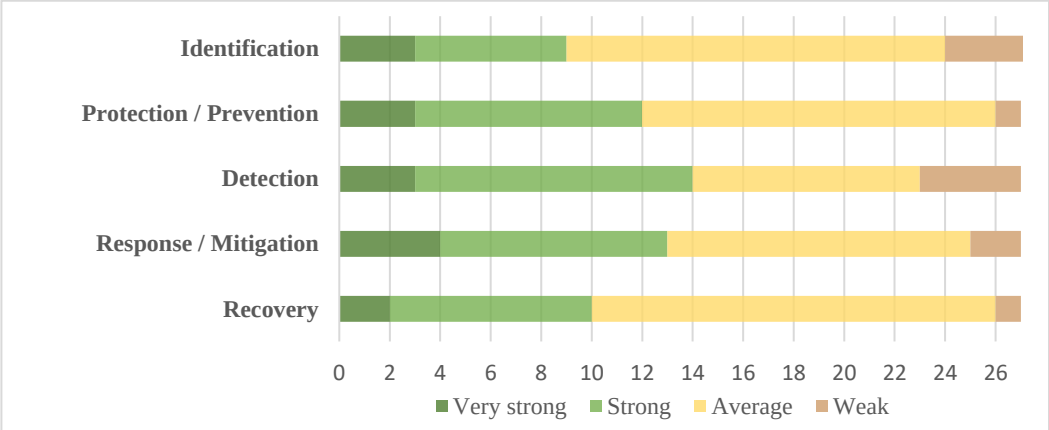
21. **Growing realization that cybersecurity requires attention.** In recent years, there has been a growing, if uneven understanding within United Nations system organizations that cybersecurity requires attention. The exposure and attractiveness of United Nations system organizations as a target for cyberattackers is undisputed, although it may vary depending on their mandate or visibility. It can be argued that the mandate or business model, as well as the information owned or managed, have influenced the pace at which organizations have recognized cybersecurity as a matter of importance. Organizations handling politically sensitive data with implications for international security or national or economic interests, as well as those managing large volumes of legally sensitive data, including the personal data of mostly vulnerable beneficiary populations, appear to have embarked earlier on the journey of upgrading their cybersecurity preparedness, while organizations with relatively non-controversial mandates have caught up with building cyberdefences at a more moderate pace. In addition, some organizations that have come into the focus of public attention due to the topicality of their mandates have had to step up their efforts significantly at short notice (such as the World Health Organization (WHO)), as have those organizations where large-scale or high-visibility cyberattacks have accelerated the need for prompt action and fortification of their cyberresilience (such as the International Civil Aviation Organization (ICAO)). Overall, however, there is no JIU participating organization that has not, in some form, recognized the importance of maintaining a solid cybersecurity posture commensurate with its operational requirements.

22. **Different maturity levels among United Nations organizations.** While no JIU participating organization was found to have been oblivious to the necessity of investing in its cybersecurity, significant differences were observed in the approaches that the various organizations had taken in their response to cyberthreats. The level of maturity of the United Nations system organizations' cybersecurity frameworks was found to vary significantly even in the absence of common benchmarks or uniformly used criteria that could facilitate a methodologically reliable, evidence-based comparison. These differences can be explained by reference to: the setting in which each organization operates; the requirements dictated by the type of data held; the level of understanding and the priority accorded to cybersecurity by the leadership; the availability of resources; and the disparity of information technology systems, tools and software solutions used, often reflecting years of uncoordinated investment decisions and vendor choices across the system. Despite structural and other commonalities that undoubtedly exist across most if not all organizations examined by JIU, attempts to provide a definitive assessment of the overall cybersecurity maturity of the United Nations system as a whole would not have done justice to the diversity that characterizes its membership. It was furthermore considered to be of limited practical value, as comparisons with other organizations or a system-wide "average" maturity would give little indication about one's own protection.

23. **Responses collected suggest room for improvement.** In an attempt to provide an approximative snapshot of the status quo, figure II illustrates how participating organizations self-assessed their overall cybersecurity framework against broad categories of functional domains, as defined in the JIU questionnaire. Noting obvious challenges in interpreting the responses received in the absence of a common reference framework or benchmark for comparison, the overall picture nevertheless does not suggest a confident cybersecurity posture across the system as a whole, even in subjective terms. The United Nations International Computing Centre, in its own assessment of the United Nations system organizations' overall performance in response to the same question, and to the extent that it was in a position to provide insight regarding its clientele, gave ratings ranging from "average" to "weak", which further confirms that there is room for improvement on a system-wide level.

Figure II

Self-assessment regarding performance in broad cybersecurity domains, by type of controls and number of Joint Inspection Unit participating organizations



Source: JIU questionnaire 2020.

Note: The categories for self-assessment were conceptually inspired by those used in recognized reference frameworks and standards in the field of cybersecurity. The cybersecurity domains referred to in the JIU questionnaire are broken down as follows: identification (critical processes, assets, resources, risks, etc.); protection/prevention (access management, awareness, training, procedures, technology, etc.); detection (anomalies and events, continuous monitoring, detection process, etc.); response/mitigation (planning, communications, analysis, mitigation, etc.); and recovery (planning, restoring, communications, improvements, etc.).

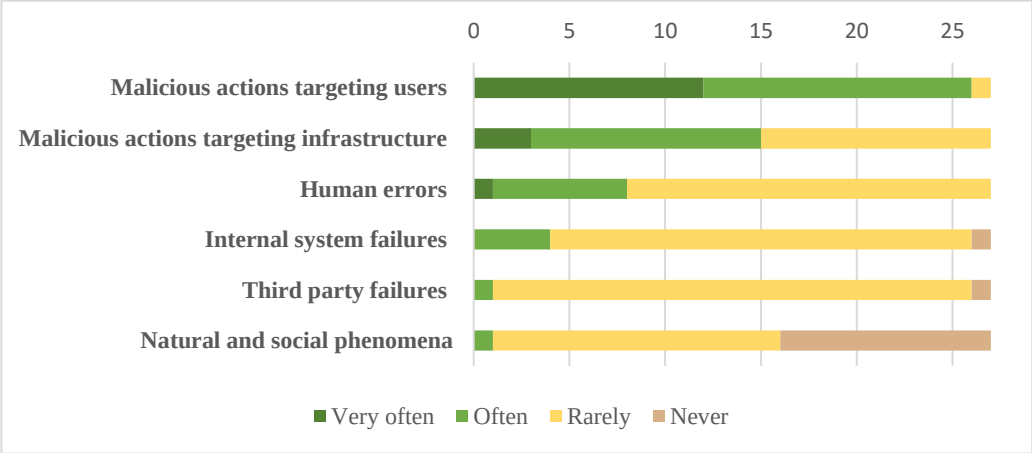
24. **System-wide risks augmented by weak individual posture.** The question of the adequate level of cybersecurity preparedness goes beyond individual organizations' respective exposure. During the interviews, cybersecurity experts confirmed the view that an organization with vulnerable or weak defences represented a risk for the other entities of the system. Once an attacker secures administrative privileges and gains deeper access to one organization's information systems, such access can be exploited to penetrate another entity's digital territory. Malicious lateral movement from one organization to another (known as "pivoting") may also be more difficult to detect and counter, because it can appear as normal traffic. Based on the information gathered in the context of one organization's infrastructure, hackers may further adapt the method of attack and deploy a more tailored set of techniques and tools to achieve their objective. Therefore, organizations assessing themselves individually as "weak" represents a collective problem. It could thus be said that the United Nations system is as strong as its weakest link. This dimension is further explored in chapter IV of the present report.

B. Cybersecurity threat landscape

25. **Most prevalent sources of threats and means of attack.** Providing an overview of the current exposure to cybersecurity threats, figure III reflects the responses provided by JIU participating organizations regarding the frequency of incidents affecting them in the last five years, categorized by threat source. Malicious actions targeting either users of information systems (through phishing, identity theft, "man in the middle" schemes, etc.) or infrastructure (malware, distributed denial of service attacks, etc.) were by far the most prevalent types of threats reported. Officials interviewed confirmed that malicious acts targeting end users were the most common and fastest growing type of attacks in the recent past. This was reinforced by the pandemic situation, which forced many end users to work from remote locations, often using private equipment that, in many cases and to varying degrees, put additional strain on corporate cybersecurity protection measures (paras. 39–41).

Figure III

Exposure to cybersecurity threats in the last five years, by category of threat source and number of Joint Inspection Unit participating organizations



Source: JIU questionnaire 2020.

Note: The threat sources were further described as follows: malicious actions targeting users (phishing, identity theft, "man in the middle" schemes, etc.); malicious actions targeting infrastructure (malware, distributed denial of service attacks, other technical actions, etc.); human errors (configuration error, operational error, non-compliance with procedures, loss of equipment, etc.); internal system failure (device or system malfunction or hardware failure, power supply failure, communications link failure, etc.); third-party failures (Internet service providers, power grid, remote device management, etc.); and natural and social phenomena (flood, earthquake, bombing, civil unrest, fire, etc.).

26. **Increase in social engineering attacks, particularly during the COVID-19 pandemic.** While cybersecurity threats are commonly associated with sophisticated technical operations targeting infrastructure, the United Nations cybersecurity community reported a discernible shift from hackers attacking servers, networks and end point devices to hacking people by using social engineering techniques aimed at manipulating individuals into divulging sensitive information for fraudulent purposes. The COVID-19 pandemic exacerbated the risks related to social engineering. More than two thirds of the participating organizations reported a sharp increase in cybersecurity threats and vulnerabilities during the global lockdowns that effectively disconnected many users from centrally managed cybersecurity resources, making contact with trained professionals for advice on suspicious emails and websites less direct due to the sudden move to remote working. According to the United Nations International Computing Centre, cybercriminals and adversaries further took advantage of the confusion and increased interest in pandemic-related content by sending COVID-19-themed phishing emails and creating fake websites loaded with malware purporting to provide information on the disease. Phishing attacks were particularly successful during this time, which was further marked by unprecedented levels of misinformation being spread, sometimes with an exploitative intent.

27. **Specific challenges related to social engineering techniques.** Unlike infrastructure-focused attacks, which directly target a limited number of computing resources that might be easier to protect, social engineering is considered challenging in several respects. While technically simple to apply, such techniques are designed to reach a high number of users simultaneously, maximizing the likelihood of a breach. In addition, even though social engineering targets end users, they are often only the entry point that provides a pathway to other critical assets. Intrusions unknowingly facilitated by members of the workforce can go undetected for years, providing adversaries extended access to internal security architecture and confidential information, which in turn offers further opportunities for attack. This may include pivoting, a technique used to move laterally from one organization's cyberenvironment to that

of another after initial penetration, taking advantage of shared or linked infrastructure. This latter tactic is of particular concern to United Nations system organizations, many of whom share common premises, data centres or servers, as it renders the defences of even the most advanced and well-protected organizations as vulnerable as those of the weakest link in the chain. It is therefore particularly important to ensure adequate training and awareness among the entire population of users so as to reinforce healthy practices.

28. **Other threats.** The organizations have also identified human errors as a non-negligible source of vulnerabilities involving configuration errors, operational errors, non-compliance with procedures, loss of equipment or inadvertent damage caused by lack of awareness more broadly. Third-party failures reportedly rarely occur, which is encouraging as it indicates that organizations appear to apply sufficient due diligence in selecting their commercial partners. Natural disasters as well as other hazards, including disruptions caused by conflict or terrorist activity, were reportedly least prevalent, yet they constitute an important area where physical security and cybersecurity considerations must go hand in hand to mitigate impact.

29. **Origin of the threats.** In the United Nations context as well as in general terms, cybersecurity incidents can originate from a wide range of threat actors (box 2), who can be internal or external to the entity, and who may act voluntarily (deliberate attack) or involuntarily

Box 2: Main types of threat actors in the cyberenvironment

- **Hackers**. Individuals or groups who break into networks to cause disruption, harm or chaos mostly for fame or for the thrill of the challenge.
- **Hacktivists**. Hackers with a specific motive who see their activity as a form of civil disobedience or as a means of political or ideological self-expression.
- **Cybercriminals**. Actors who engage in cyberenabled criminal activity (common crimes such as fraud, theft, extortion etc., aided by computerized means) or cyberdependent criminal activity (e.g. deployment of viruses or malware and other activities that can only be committed through computerized means). According to the level of technical sophistication and organizational capacity, the actors involved can range from small outfits to large, organized crime networks.
- **Industrial spies**. Sometimes considered a subcategory of the criminal group, the goals of these actors are specific in obtaining trade secrets, blackmailing for reasons of economic interest, or sabotaging the competition, and they are mostly encountered in the corporate world.
- **States or State-sponsored groups**. Highly sophisticated, well-resourced actors whose activities tend to be difficult to detect, trace or identify and who may pursue complex, often indirect and non-evident objectives in a stealthy manner, directly employed by or indirectly financed by governmental or military outlets. In the past, States had developed primarily investigative capabilities, but in recent years it has become a widely accepted fact that some have additionally acquired offensive capabilities.
- **Insiders**. Actors who, by virtue of a contractual relationship with the organization concerned, are not considered external but endanger the entity from within. This may include disgruntled employees and poorly trained personnel or contracted service providers, among others.

(by inadvertent actions or omissions or by being instrumentalized without their knowledge). Some criminal groups offer their capabilities to other actors for hire, effectively outsourcing attacks through a practice that can be termed “cybercrime-as-a-service”. Accordingly, the

question of who is behind a particular attack (threat attribution) is challenging to answer, not least because of the myriad mechanisms that exist to obfuscate the actual source of the attack (e.g. through spoofing, bot herding, etc.). Indeed, a number of officials interviewed admitted that United Nations system organizations were not only lacking the capacity to reliably determine the origins of an attack but were also reluctant to pursue attribution, as the costs involved in attempting to do so far outweighed the benefits or utility of knowing who was behind the intrusion. Many expressed that they focused their efforts on prevention, detection and response rather than investing time and resources into pursuing adversaries, since doing so would take considerable efforts, and even if the adversaries were successfully stopped, it would not solve the problem as organizations would continue to face new ones. This also holds true for the phenomenon of advanced persistent threats, which were confirmed by organizations to be a non-negligible occurrence and tended to take the form of intrusion, monitoring and delayed action requiring a level of resources and sophistication commonly associated with State-sponsored attacks.

C. Known and unknown impact of cybersecurity incidents

30. **Limited impact reported.** To better understand the extent to which risk has translated into cybersecurity incidents that have affected its participating organizations, JIU asked them to rate the impact of past incidents by severity (from insignificant to severe) and category of impact (financial, operational, digital, political or reputational, material or physical, or productivity related). Interestingly, and perhaps surprisingly, in their responses participating organizations invariably reported the impact of cybersecurity incidents they had been confronted with as minor or insignificant, irrespective of the impact type. At the same time, it is acknowledged that the number and frequency of averted cybersecurity incidents is considerable, in the range of thousands of events per month, and has grown exponentially in recent years. This is telling about the volume of cyberthreats to which organizations and their infrastructure are exposed today. Yet, at first glance, and keeping in mind the relative absence of systematic data collection in this regard, it appears to suggest a relatively limited impact overall.

31. **Most affected areas.** The organizations reported that the areas most affected by cyberattacks (the impact was rated as "moderate" by a comparatively larger but still limited number of organizations and "major" by one or two organizations but "severe" by none) had been the digital realm (mainly data leaks) followed by political and reputational damage (misinformation, unfavourable media attention, undue interference in intergovernmental processes, etc). Even in financial terms, the direct losses (such as fraudulent transfers of funds) involved only small amounts, cautiously suggesting that control measures had been effective in that regard. However, the Inspectors wish to highlight other associated financial consequences of cyberattacks (e.g. staff time and costs involved in investigating what happened and determining the extent of the damage caused, costs of recovering assets or equipment, consultancy fees for external capacities required to resolve breaches, productivity loss during system downtimes, or the costs of investments towards the prevention of future problems), which may be far more complex to quantify but are undoubtedly significant. Overall, despite the fact that the majority of participating organizations self-assessed their cybersecurity response capacity as "average" (only a third considered it to be "strong" or "very strong"), the impact of cybersecurity incidents experienced by the United Nations system today, as reported, did not in itself suggest a serious cause for concern.

32. **Reality unknown.** However, several factors suggest that priority attention to cybersecurity is warranted. First, the data collected imply some blind spots, confirming that the exact magnitude of the threat and related consequences are not known, as acknowledged by several organizations in their responses. Most of the time, especially in the case of more sophisticated attacks, adversaries have no incentive to reveal their presence nor the vulnerabilities they exploited, which suggests that undetected system breaches and data leaks are likely to be significantly above the reported level. In this context, several interlocutors

pointed out that the proportion of "known unknowns" compared to what was known about the magnitude of the cybersecurity threat was large, but the share of "unknown unknowns" might be of even greater concern. Second, responses may (intentionally or unintentionally) minimize the impact, given that, in a corporate culture driven by performance-related reporting and an acute sense of dependence on resources tied to such reporting, honest acknowledgment of weaknesses has yet to become the norm as part of the organizational culture. This may skew findings accordingly. To give an example, in their response to the JIU questionnaire, 11 participating organizations officially confirmed having experienced at least one major cyberattack that had an impact on their operations in the recent past. However, there are entities that are known to have suffered such attacks as a matter of public record yet did not disclose this in their interactions with JIU. One can therefore assume that the actual threat as well as its impact exceed both what is known and what organizations may be prepared to divulge.

33. **Past threats are no indicator for future incidents.** Notwithstanding the above, there appeared to be consensus among experts that judging the seriousness of the threat by the extent to which it was known to have materialized in the past would be misguided. The potential for damage remains high and should be anticipated with counter-strategies readily in place. For example, the growing threat of ransomware being deployed for purposes of extorting money in exchange for stolen data seems to have spared United Nations system organizations until now, with some exceptions. Media reports confirm that several well-known entities, including large private sector companies and even local government entities, have been forced to pay ransoms to regain access to their data and information systems. The Inspectors note that, presently, there is a clear stance taken by participating organizations against paying any ransom to criminals. In the same vein, it is worth noting that, at this point in time, United Nations system organizations did not report having experienced any cyberattacks against connected devices, such as elevators, ventilation systems, autonomous vehicles or similar remote-controlled equipment. Targeting connected devices is an emerging area of cybersecurity risks, but entities should be attentive as industry experts forecast a significant increase in this type of threat in the future. These two examples show the importance of anticipating risks for which there may have been limited precedent in a United Nations context so far, and of proactively integrating cybersecurity considerations into the overall risk management process of the organizations.

34. **Cyberinsurance.** To increase proactive protection against emerging threats, one option is to purchase cyberinsurance to cover the damage caused by cyberattacks, as well as, arguably, to escape having to deal with the ethical dimension of the question of whether or not to pay a ransom. Commercial vendors, on a case-by-case basis, might be required by their client to provide cyber insurance. During the review, no United Nation system organization indicated that it had opted for such insurance covering cyberrelated risks, though some indicated that they had been considering it. Acknowledging the prevalent position among United Nations entities, the Inspectors do not consider cyberinsurance to be an effective instrument for proactively counteracting related risks in most operational contexts, particularly as it would only be a partial mitigation strategy contributing to the minimization of financial losses a cyberattack might cause, while achieving little in terms of addressing operational or reputational damage. However, **in the Inspectors' opinion, executive management is well-advised to prepare for the eventuality of such threats, which are likely to increase in the future.**

D. Engagement and cooperation with national authorities

35. **Uneven practice and limited appetite for reporting to national authorities.** Participating organizations have different practices when it comes to reporting cybersecurity breaches to national authorities that might be in a position to investigate and take administrative or judicial action in respect of a cyberattack. About one third of the participating organizations stated that they reported incidents to national law enforcement authorities, yet few did so systematically or routinely. Among the organizations that indicated having engaged with national authorities on cybersecurity matters in the past, most confirmed having done so on a

case-by-case basis rather than acting based on organizational policy or established practice. Many used informal working level relationships rather than formal channels where possible, and only in the event of significant attacks that suggested either a likely impact on the host country or a significant reputational risk for the organization. Even in cases where investigative capabilities at the national level would exceed and could thus helpfully complement internal – often very limited – capacities to pursue suspected attackers, few organizations expressed a desire or need to formalize or increase systematic interaction with national authorities on account of cybersecurity breaches. The overall picture suggests that the appetite for engagement with national authorities is limited and that the preference is to keep interaction informal and "as necessary".

36. **Factors influencing organizations' practice.** There are various factors that may lead organizations to hesitate before contacting national authorities. One is the legal status of the organizations as bearers of privileges and immunities as such, especially in relation to the confidentiality and inviolability of their data, which must be free from any interference of a legislative, executive or judicial nature. The boundaries of legal obligation in this sphere are often poorly understood by cybersecurity practitioners. In fact, while States are under legal obligation to offer protections, organizations are only under duty to cooperate with national authorities to the extent that such cooperation does not interfere with their ability to exercise their functions independently. Such cooperation is thus always voluntary. This formula may indeed be a fine line to navigate in practice but should not hinder voluntary collaboration where warranted, and after the possible risks of collaboration have been fully assessed. In any case, there is no duty to report incidents to national authorities or divulge any data that are considered sensitive. Legal departments are best placed to advise decision makers in this regard. Another consideration in deciding whether to contact national authorities or not may relate to the maturity of the respective country's own cybersecurity apparatus, as well as its handling of cyberoffenders once referred to national jurisdiction. Such concerns may be compounded in cases where the organizations' own staff are implicated in endangering the cybersecurity of the organization (insider threats). In such cases, the standard procedure foresees lifting the privileges and immunities and handing over the person to his or her State of nationality for further investigation and possible prosecution. However, this remains a comparatively rare occurrence, particularly for cybermisconduct. Since 2007, when related statistics started to be compiled and published, only one case of staff misconduct that has been referred through the Office of Legal Affairs to national authorities for further investigation involved a breach of information security.[11] Beyond the considerations elaborated above, the severity of the incident, the utility and probability of succeeding in attributing attacks to a particular perpetrator, the potential for undue exposure of confidential or sensitive information, and the possible impact of an investigation on operational activities were among the most frequently cited considerations to weigh when deciding whether or not to reach out to national authorities. Some officials also acknowledged that reporting to national authorities was often simply neglected as an option.

37. **Decision-making process to report to national counterparts.** As shown above, the decision on whether or not to initiate contact with national authorities involves dimensions that go beyond the remit of cybersecurity experts. A combination of political, legal, evidentiary and practical considerations is at play, and such a decision should therefore involve a range of stakeholders. In organizations where the Inspectors found evidence of a more established approach to engagement with national authorities, the distribution of responsibilities mirrored the spectrum of considerations involved, which was found to be a good practice. More specifically, the affected programme office or substantive unit would assess the severity of the intrusion, weighing the programmatic risks and benefits of contacting national authorities. The legal office would assess and advise on possible ramifications of a legal nature given the special status of organizations and their staff in the jurisdictions concerned, including the possible need to lift privileges and immunities and, where applicable, refer implicated staff to their country of nationality. The role of the ICT department or the cybersecurity experts would be to provide

[11] A/75/217, annex I.

forensic evidence of the breach to the extent available. The decision on whether to proceed with raising the matter with the host country would rest with the executive management, with input from all of the above-mentioned stakeholders. Once a decision has been made to engage national authorities on account of an incident, the mechanisms for doing so are normally the established lines of communication between the relevant offices of the United Nations organizations, the permanent mission of the State concerned and the relevant authorities of the host country concerned. Given some critical observations made about the effectiveness of the established process, there may be scope for studying some alternative or complementary avenues, some of which are described elsewhere in the present report (paras. 161–163).

E. Technological preparedness – select issues for attention

38. **Basic technical capabilities well-developed, areas for closer attention highlighted.** The Inspectors put a series of questions to the participating organizations with the aim of examining the overall state of their technological preparedness to fend off cyberthreats. In doing so, the intention was not to conduct a comprehensive assessment of the robustness of their operational arrangements or their technical infrastructure, but rather to gain an understanding of the general capacities in place and isolate some common issues that might deserve special attention. Keeping in mind the limitations inherent in information gathered primarily through self-assessment, as well as the considerable variation in the level of detail shared with the Inspectors, the responses indicate that participating organizations consider the core technical aspects of cybersecurity to have been well understood and invested in, in accordance with their own respective abilities. For example, two thirds of the participating organizations indicated having network monitoring tools in place. In addition, most organizations indicate that they have set up firewalls or other intrusion prevention systems, while 13 organizations report having implemented a Security Information and Event Management system. It is in areas that have been subject to more dynamic technological development in the recent past that the picture appears more nuanced and may warrant some attention by participating organizations. In this section, for security reasons, specific organizational arrangements are not identified, so as to avoid conclusions that could jeopardize the security of the entities concerned.

End point device management and tools facilitating remote work

39. **COVID-19 pandemic brought management of end point devices into focus.** The pandemic forced the implementation of alternate and flexible working arrangements on a much larger scale than practised before across almost all occupational groups, both at headquarters and in the field. Against this backdrop, organizations' ability to operate off site, with limited physical access to premises and centrally connected computing equipment, has been subjected to an unprecedented stress test, and tools facilitating remote work have come under increased scrutiny from a cybersecurity perspective. On the one hand, this includes employees' ability to securely access computing resources remotely, which two thirds of the organizations indicated that they were facilitating through the use of virtual private networks, with the remaining organizations using cloud-based services that were accessed via encrypted Internet protocols over the public network without requiring virtual private networks. On the other hand, the ability to operate off site involves the management of end point devices (desktop and mobile computers as well as other mobile devices), for which the responses indicate a more varied level of coverage.

40. **End point device management lagging behind.** While the majority of organizations mention some degree of centralized device management, a number of them do not appear to provide complete coverage. In some cases, coverage is limited to equipment located at headquarters only, with seven organizations noting that their field offices follow separate device management practices, and in other cases, only permanently connected computers are covered centrally, while about a third of the participating organizations neither manage nor protect

mobile devices centrally at all, even though a few are in the process of rolling out platforms for this purpose or plan to do so in the near future. Only two responses mention end point device encryption, which is an important measure for preventing data theft and leakage, particularly at the level of end user portable devices, which are generally more prone to loss and theft. Responses provided evidence that organizations were aware of the need for enterprise device management but showed that mobile device management was lagging behind. Existing vulnerabilities in this regard were rendered more acute by the use of personal, non-corporate mobile devices such as private laptops – a practice that has seen a significant surge during the pandemic.

41. **Important cybersecurity measures introduced or sped up.** Despite many challenges encountered, the advent of the pandemic also prompted some positive developments. United Nations entities were pressed to take a closer look at their security management frameworks, and planned corporate ICT projects started to materialize, driven by immediate necessity. It can be said that the massive switch to remote working at very short notice led many organizations to accelerate their efforts towards improving remote access security and, judging by the responses to the JIU questionnaires, may have provided a much needed impetus to galvanize action in this regard. In fact, most entities put in place a multi-factor authentication system for remote access purposes, rolled out tools for online collaboration and data sharing at previously unmatched levels, further institutionalized the use of electronic signatures and scaled up information security training opportunities. In a sense, the pandemic became a catalyst for the ICT transformation of several United Nations entities and pushed them in the direction of digitalization and advanced digital working practices – a factor having implications not only for the field of cybersecurity, but also, in much broader terms, for the way organizations work, as well as the way assets and premises are managed.

Legacy systems

42. **Specific vulnerabilities created by legacy systems.** Several participating organizations pointed out that the upgrading or retirement of ageing legacy systems that might no longer be supported by state-of-the-art applications was posing significant cybersecurity challenges. The continued presence of such legacy systems was said to represent a major source of vulnerability, as many of them were designed to be used only locally, on private – local or wide area – networks, which had been considered safe environments. Mainly due to the evolution of remote access and the increased use of cloud computing, these applications are now much more exposed to risks emanating from the greater interconnectedness of systems and data more globally, while not being built to resist more contemporaneous forms of attack. Some of the vulnerabilities created as a result might be registered and signalled by vulnerability management systems, but the possibility remains that some proprietary legacy applications would not be automatically detected. Even when detected, they may not necessarily have immediate fixes and can lead to unduly extended exposure of the entities concerned. In addition to the risks for the legacy applications themselves, such vulnerabilities also present a risk for other applications and data that may share the same infrastructure, as the former can be used for lateral movement across systems and applications once compromised.

43. **Careful review of legacy systems warranted.** It is therefore important that the United Nations system organizations keep track of and actively work on upgrading or replacing such systems. Considering that some of these legacy systems are large and complex (such as enterprise resource planning systems), and that many were custom-built in-house over long periods of time, this task may be complex for many, requiring further financial resources and efforts to obtain and sustain the buy-in of the business units that had invested in the development of tailored solutions now considered unsafe. **The Inspectors suggest that executive heads, in close cooperation with ICT and cybersecurity experts as well as affected business units, launch a careful review of the issue of legacy systems within their organization unless already initiated.** Cybersecurity considerations should feature prominently in their analysis, on par with the strategic and timely consideration of resource

implications and the immediate and longer-term impact of the decommissioning of such systems on operations, which should be addressed through adequate planning for the institution of temporary mitigation measures, where possible.

Cloud security

44. **Protection offered by external cloud computing service providers improved considerably according to cybersecurity expert community.** Since 2019, when JIU released its report on cloud computing,[12] both the use of cloud-based services by its participating organizations and the scope and maturity of such services have seen considerable growth. Their ubiquity, elasticity (the ability to continually match the allocation of computing resources with actual resource demand in real time) and cost effectiveness, as well as their ever-growing technological sophistication, have inspired users' trust in their sturdiness and safety, further increasing their attractiveness for the United Nations system. Organizations continue to migrate their existing applications to cloud-based services, and the decision to do so remains organization-specific. In this regard, the Inspectors acknowledge the increasing recognition across the cybersecurity expert community that the cloud computing capacities and assurances offered by commercial industry leaders today exceed the level of data security, confidentiality and cyberresilience they were able to provide just a year or two ago. According to the experts, the protections currently offered by such providers are also likely to exceed the capacity of any one organization to achieve a comparable degree of security using in-house developed solutions. There was only one example encountered during the present review in which a participating organization was found to have opted to detach completely from cloud-based solutions for a discrete, particularly sensitive portion of the data it managed. However, it is worth noting that this choice was made for a limited data set and was predicated on that organization's capacity – including financial capacity – to provide a viable alternative, which is not a given for most organizations.

45. **Continued vigilance in using external cloud computing services warranted.** Even against the backdrop of the significant advancements made in recent years regarding the security of cloud computing, the recommendations to executive heads made in the referenced JIU report remain valid as regards the following: the need for the alignment of cloud computing services with business needs to provide value for investment; comprehensive risk assessments and careful vendor management in the engagement of external cloud service providers; and strategies to mitigate the risk of vendors' potential failure to provide the contracted services. The concerns regarding risks of monopolization and excessive concentration of United Nations data in the hands of comparatively few technological giants also continue to persist. Accordingly, organizations cannot afford to let down their guard when using cloud-based applications or deploying their applications and data in the cloud, particularly considering the risk of unauthorized access to confidential or sensitive data. They must continue to exercise due diligence and maintain sound cybersecurity practices when relying on cloud computing services, in particular by requiring evidence of their providers' compliance with independent audit requirements and the production of relevant certificates, such as System and Organization Controls reports, in particular the ones known as "SOC 2 reports", or similar assurances that are widely recognized by industry experts. Demanding such external, independent assurance becomes important when considering the fact that the competence of internal audit and other organizational oversight mechanisms may cease when external providers are engaged. It is thus recommended that the view of the internal audit department be sought when entering into a contract for such services, so as to ensure that relevant provisions are included to provide reasonable assurance of compliance with appropriate internal control standards regarding the collection, storage and use of the information provided. Consultations with the legal office are also advisable. Organizations must therefore find acceptable alternatives to assert a degree of control that is considered adequate, for instance by including provisions into contractual arrangements with external cloud service providers that permit the entity to exercise oversight

[12] JIU/REP/2019/5.

and control over compliance. Furthermore, commercial cloud-based facilities can change owners, even across borders, which may, in some contexts, further exacerbate the risk of exposure of the data held or managed by such facilities in the event of attempted legal proceedings in the respective national jurisdiction. In such situations, privileges and immunities would be asserted and maintained in respect of all data held on behalf of United Nations system organizations. However, organizations must remain vigilant and take the necessary precautions to manage such risks as much as possible.

46. **Zero risk unattainable, detailed analysis required.** Irrespective of the cost efficiency and security benefits to be gained, the Inspectors recall that both cloud-based solutions and traditional data centre approaches are exposed to cybersecurity threats and can never claim to be impenetrable. It is therefore unrealistic to strive for a complete elimination of risks in either environment. Regardless of whether the risk is, to a degree, transferred to external entities who manage the related computing environment, the accountability for the consequences of cyberattacks remains internal. Accordingly, organizations are well advised to engage in a detailed analysis before deciding whether they are prepared to entrust the protection of their information to third parties, and if so, which aspects. In that spirit, data protection assessments should ensure that the safeguards of the cloud computing services are in line with the organizations' requirements and commensurate with the type and sensitivity of the data assets concerned. Similar considerations apply to any decision about outsourcing and are therefore not limited only to the context of using cloud security.

Vulnerability management

47. **Uneven practice across participating organizations.** Vulnerability management is considered to be one of the major cybersecurity challenges in international organizations today. New vulnerabilities in widely used software are being discovered almost daily, including the software used by United Nations system organizations. While device and software vendors constantly develop and make available corresponding patches, these translate into a considerable amount of information to be processed and involve significant workload in applying the patches in complex technical environments. To deal with this challenge, more than half of the participating organizations reported having some form of vulnerability management solution in place. For example, some use subscriptions to multiple intelligence feeds to continuously learn about (and defend against) new threats, including new vulnerabilities, while others have chosen to deploy integrated security solutions sourced from commercial providers that include vulnerability management. Detecting and patching vulnerabilities was highlighted by some organizations as a demanding cybersecurity activity. Some observed that malicious attempts to find vulnerabilities in their networks and systems were increasing with time, while the distributed nature of their ICT network made it difficult to centrally manage the vulnerability patching process, in particular across multiple field locations. Several organizations also reported that vulnerability patching expenses featured among the most significant costs associated with their cybersecurity programmes.

48. **Continuous vulnerability management to be pursued.** The Inspectors draw attention to the fact that there is a significant difference in effectiveness between ad hoc (for example, annual) vulnerability assessments and a continuous process of vulnerability management and patching. If patches are not regularly applied, then ICT systems remain exposed to malicious exploits for too long, and the risk of compromise grows considerably. Information collected from participating organizations in this regard did not provide a sufficient level of confidence that this challenge was being addressed in an adequate and consistent manner. Responses to the JIU questionnaire from several organizations rather suggest a more ad hoc approach to vulnerability assessments (conducted either annually or even more infrequently), while other organizations such as the United Nations Relief and Works Agency for Palestine Refugees in the Near East (UNRWA), the World Food Programme (WFP), ICAO and the United Nations Educational, Scientific and Cultural Organization (UNESCO) count effective, continuous vulnerability management among the good practices in their organizations. **There is room for**

improvement in this area, and the Inspectors urge executive heads to accord sufficient attention and adequate resources to enable the conduct of regularized vulnerability assessments, with a view to establishing vulnerability management as a systematic exercise in the United Nations system organizations.

Shadow information technology (shadow IT)

49. **Reasons for resorting to shadow IT.** The term shadow IT refers to ICT applications or solutions developed or adopted inside an organization but outside of its official, usually centrally managed ICT framework. Most often, shadow IT is a result of users trying to solve a practical problem using tools that are readily accessible on the market at low or no cost, when the solutions available through the established channels and structured ICT capacities may be perceived as not meeting their needs in terms of timeliness, cost or customization. It can also result from a desire to rapidly innovate in response to evolving needs or to ensure alignment or compatibility with tools used by implementing partners that may not coincide with an organization's corporately sanctioned choice. Examples include opening free accounts with service providers offering data storage, file transfers, web design or content management solutions, or developing applications in-house for use by individual departments or field offices or in a project setting. These solutions are not normally or not necessarily vetted for compliance with the cybersecurity policies and procedures put in place by the official, centralized authority at corporate level and thus may be considered to operate in a non-authorized, "shadow" environment.

50. **Risks associated with the use of shadow IT.** In some organizations, the phenomenon was said to have proliferated, particularly in field offices or departments that were further removed from central control in other ways. The risks in such settings are often amplified by the central ICT and cybersecurity departments having limited insight into individual ICT development activities. Again, the COVID-19 pandemic, by creating a sudden need to perform many functions remotely, further accentuated this challenge as many users started to use tools for online collaboration, including conferencing, outside of the solutions provided through the corporate software packages. However, many of the services to which users resorted as potential alternatives had not been evaluated or cleared by organizations' cybersecurity experts for mass usage, potentially putting the organizations at risk (for example, by adhering to different standards than those recommended at the entity level with regard to authentication or confidentiality). For example, the use of a popular online videoconferencing platform was studied by the Information Security Special Interest Group in the early days of the pandemic to assess its adequacy for use by United Nations system organizations, yet the cybersecurity experts could not arrive at a conclusive and unequivocal – positive or negative – recommendation that could be considered valid for the system as a whole. Instead, they formulated a range of options along with caveats and precautionary measures to consider when using the online platform in specific settings.

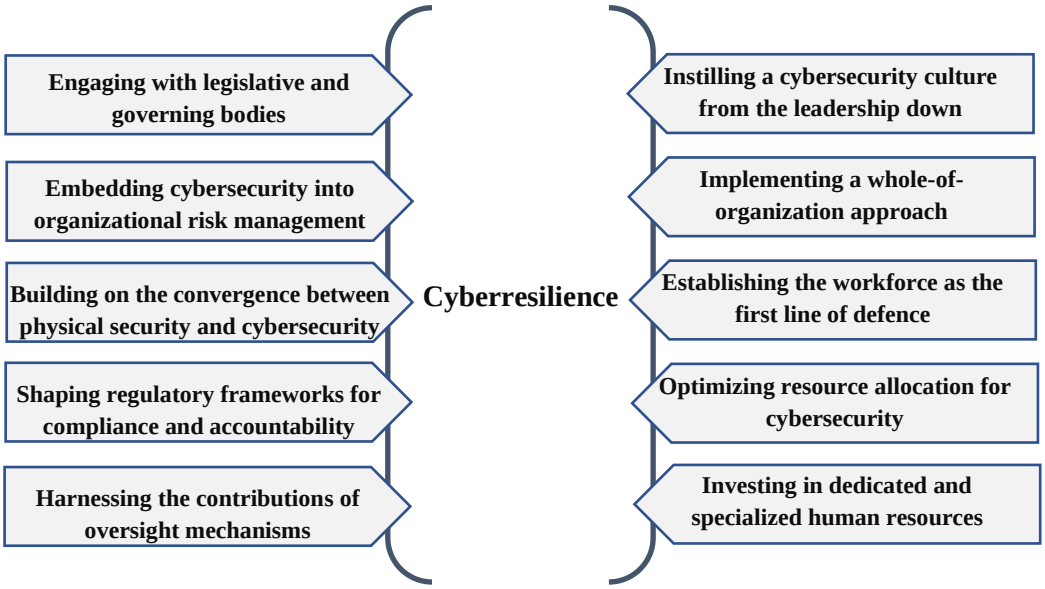
51. **Some suggestions for more attentive shadow IT management. The Inspectors consider that cybersecurity challenges related to shadow IT practices need more attention, balancing the need for control in an environment that is prone to cyberrisks against the legitimate needs and constructive motivation of users to innovate and to avail themselves of alternative solutions where available.** In fact, a case was made not to automatically dismiss as undesirable behaviour some users' impulse to reach for shadow IT solutions, as it was considered a healthy sign of a readiness to innovate, for which business units should generally be allowed some space and capability, ideally in a safe and guarded computing environment. Ideas to harness to that effect include: creating or expanding secure environments for digital innovation; improving the visibility of distributed ICT development occurring in more decentralized settings through local ICT focal points; and enhancing end user training and awareness-raising measures to include solid and clear information on the security and risk aspects of using third-party services outside standard procedures and practices, along with

information about approved corporate alternatives, as well as recommendations for safer use of such solutions.

III. Elements contributing to improved cyberresilience

52. **Cyberresilience as a corollary of a culture of cybersecurity**. In addition to technological preparedness involving the identification of digital solutions and data sources for the protection of corporate resources, a strong cybersecurity posture results from a multifaceted approach that involves all levels of the organization, including legislative and governing bodies, oversight mechanisms, executive management, substantive or business units and programme managers, the workforce at large, as well as implementing partners and external service providers. In other words, a whole-of-organization approach is indispensable to creating the conditions for improving cyberresilience. In addition, cybersecurity cuts across several organizational domains and competences, including ICT, risk management, physical safety and security, and information and knowledge management more broadly. The multiplicity of considerations and the awareness of all stakeholders regarding their role and contribution to successfully raising the bar for the cybersecurity of each organization can be referred to as components of a culture of cybersecurity that, once instituted and practised, helps attain organizational cyberresilience. In the present chapter, the Inspectors present their findings regarding the extent to which participating organizations' frameworks and practices reflect such elements that contribute to improved cyberresilience (vertical perspective), as summarized in figure IV, and suggest possible improvements.

Figure IV
Elements contributing to improved cyberresilience



Source: Prepared by JIU.

Note: Cyberresilience is defined in one leading industry standard as the ability to anticipate, withstand, recover from and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyberresources.

A. Engaging with legislative and governing bodies

Legislative and governing bodies to provide strategic guidance and resources

53. **Cybersecurity deserves legislative and governing bodies' attention.** JIU has consistently stated that legislative and governing bodies of intergovernmental organizations have a decisive role to play in providing strategic guidance and adequate resourcing for any organization's ability to deliver its mandated activities. As stated in a recent JIU report on

enterprise risk management,[13] legislative and governing bodies must show engagement and should be aware of, at a minimum, the key strategic risks an organization is facing and the strategies and frameworks in place to manage them. **In the Inspectors' view, this should include engagement and guidance in the area of cybersecurity, given its critical nature both as a risk management issue and as a key enabler of the delivery of organizations' mandates.** Concrete ways in which the respective bodies can become more engaged and support corporate efforts in this domain are suggested in box 3. However, as cybersecurity is still perceived as a predominantly technical and therefore operational rather than strategic issue, the extent to which legislative and governing bodies have been called upon to establish, or themselves called for, engagement on the topic has been limited in most organizations to date.

Box 3: Opportunities for engagement of legislative and governing bodies on cybersecurity

- Formulate an explicit statement on the risk tolerance and appetite of the organization regarding cybersecurity matters that articulates the level of risk considered acceptable in its specific context. There was limited evidence of the existence of such statements across the participating organizations, with the exception of the United Nations Development Programme (UNDP) and the World Intellectual Property Organization (WIPO), where a sophisticated and well-elaborated methodology for articulating the risk appetite had been implemented.
- Provide high-level strategic guidance on cybersecurity priority areas. A good example of such guidance is the section on "information security" embedded in the information and communications technology strategy of the United Nations Secretariat, which was endorsed by the General Assembly in 2014 (A/69/517).
- Allocate adequate financial resources based on a sound business case, as presented by executive management, which would enable the implementation of the objectives formulated in the strategic guidance offered by the legislative and governing bodies in line with the risk appetite.

54. **Legislative and governing body engagement in practice**. The depth and level of engagement with legislative and governing bodies on cybersecurity differs, depending largely on an organization's mandate and operational requirements. Few organizations have recognized, let alone harnessed, the potential of active engagement with the legislative and governing bodies on cybersecurity matters, and among those who have, most did so only after a major attack necessitated increased attention and interaction at the political level. While the format of such engagement differs, and there is no one "right" level or degree of interaction, there is already some recognition of the fact that a certain information flow between those responsible for cybersecurity within an organization and its constituent members is not only beneficial but may be necessary. Below, the Inspectors distinguish regular reporting mechanisms on cybersecurity from procedures to be followed for the escalation of incidents to the legislative and governing bodies.

[13] JIU/REP/2020/5.

Reporting and escalation mechanisms

55. **Existing reporting mechanisms.** The Inspectors found that a minority of organizations included some form of periodic reporting on cybersecurity matters to their legislative and governing bodies. Where such reporting exists, it takes different forms: (a) some organizations may include relevant information in their programme budget and performance reporting (typically as part of the ICT segment, which may or may not explicitly cover cybersecurity); (b) others engage in dedicated reporting upon request by the legislative and governing body, such as reporting to showcase progress in the implementation of endorsed or adopted strategies or road maps; and (c) yet others rely on the annual reporting of their internal and external oversight bodies, using it as the primary channel to make a case for increased attention to the subject.

56. **Cybersecurity metrics neither collected nor presented systematically**. There is also disparity as regards the content of such reporting to legislative and governing bodies, with few organizations sharing select aspects of the metrics they collect and analyse internally regarding their cybersecurity exposure and performance. On the one hand, this uneven practice in reporting may be a product of the legitimate hesitation of many organizations to create a public or even classified record of cybersecurity metrics that may reveal vulnerabilities and thereby increase risk exposure. On the other hand, it may reflect the fact that organizations are still grappling with determining the right level of detail and most relevant selection of metrics to report, as well as the most meaningful set of metrics to collect in the first place. The majority of participating organizations produce metrics related mainly to the frequency, severity or volume of cybersecurity incidents over a period of time, gathered for internal purposes, with some organizations having yet to institute or formalize more ad hoc forms of data collection in this area. However, the type of data collected and analysed varies greatly from one organization to the next, and the way in which such data are processed with a view to guiding decision-making, whether internal or at the level of legislative and governing bodies, has yet to be defined in many organizations. Since such metrics provide one of the key components on the basis of which an organization's risk appetite can be articulated, **the Inspectors consider it prudent to continue studying different sets of cybersecurity metrics in the relevant forums and to develop a basic methodology that can be adapted to the context of each organization as needed**.

57. **Escalation to and benefits of transparency with legislative and governing bodies.** In the event of a cybersecurity incident, legislative and governing bodies are not systematically informed, which is clear from the responses to the JIU questionnaire submitted by the participating organizations. In addition, the Inspectors found that there was limited evidence of processes for escalation to the legislative and governing bodies having been pre-defined for this eventuality. The decision for escalation is usually handled on a case-by-case basis. The experience of those organizations that have had the opportunity, often forced by a major cyberevent, to test their escalation and communication channels with governing bodies points to the following main factors for consideration regarding whether to escalate: (a) the severity of the incident; (b) the impact on operations; (c) the impact on intergovernmental processes; and (d) whether the incident is likely to become public. Other decisive considerations are the timing of escalation and precaution in not revealing specific vulnerabilities or details about the organization's response capacity that could attract more attention to the target. Cybersecurity experts interviewed generally considered that a good moment to escalate would be before full resolution of the incident had been achieved, or rather, as soon as a sufficient understanding had been established concerning what one was dealing with. Doing so immediately upon discovery of the intrusion may be too early and bears the risk of compromising ongoing resolution efforts, thereby inadvertently increasing exposure. At the same time, delaying escalation to the moment when the incident is completely resolved may cast doubt on the trustworthiness or willingness of executive management to act transparently and assume responsibility for possible cybersecurity loopholes. The general message from those participating organizations that had "opened up" to their legislative and governing bodies about incidents and shortcomings in their

cyberdefences was to not be afraid to communicate, as the reputational cost, also in terms of a loss of confidence on the part of donor governments, by far outweighed the possible embarrassment and damaging impact – including indirect financial impact – of an attack.

58. **Need to anticipate escalation protocols, both internally and for legislative and governing bodies. In the view of the Inspectors, it is important to define in advance the mechanism through which significant cyberattacks will be escalated to the attention of legislative and governing bodies.** Since the likelihood of such attacks can be anticipated, it follows that the escalation protocol can be too. Specifically, the criteria (what triggers escalation) and the mechanics of who needs to take what steps in which order and with whose input need not be subject to reactive decision-making. If left to improvisation at a time of acute crisis, such decision-making is more likely to be tainted by the pressure of having to exercise ad hoc damage control rather than generally following an established protocol while being free to focus on managing inevitable case-specific variables. Moreover, having to devise such steps in crisis mode would render the process more vulnerable to undue influence in an already complex and potentially politicized setting, which can be avoided to a large degree through a proactive approach. Finally, and without prejudice to the protocols for escalation drawn up by organizations internally, it may be prudent for legislative and governing bodies to consider a debate about their own rules of engagement on such matters in anticipation of serious cases of cyberattack being referred to them for deliberation and action. Such a forward-looking approach may help set some carefully considered and agreed boundaries for action taken by legislative and governing bodies that may facilitate de-politicization and sound decision-making in this potentially sensitive area.

B. Embedding cybersecurity into organizational risk management

59. **Benefits of a risk management approach to cybersecurity.** A recent JIU report characterized enterprise risk management as an organization-wide process of structured, integrated and systematic identification, analysis, evaluation, treatment and monitoring of risks towards the achievement of organizational objectives.[14] The core functions associated with cybersecurity (usually variations of identification, prevention, detection, response and recovery) mirror the key stages and objectives of risk management. Treating cybersecurity as a corporate-level risk management issue also carries concrete practical benefits. For one, being recognized as a strategic, organization-wide concern, cybersecurity becomes a matter that concerns all business units and all employees, encouraging and supporting a whole-of-organization approach and buy-in through distributed ownership of risks. **Furthermore, the Inspectors affirm that embedding cybersecurity formally in the organization's enterprise risk management framework contributes to elevating the subject among diverse organizational priorities and provides a formal point of reference, based on which legislative and governing bodies and senior management can jointly devise a path for how best to manage key risks.** Since such frameworks tend to be conceptualized as living documents, they also provide an opportunity for the systematic and recurrent reconsideration, adaptation and tailoring of risk mitigation measures in the light of rapidly evolving organizational needs.

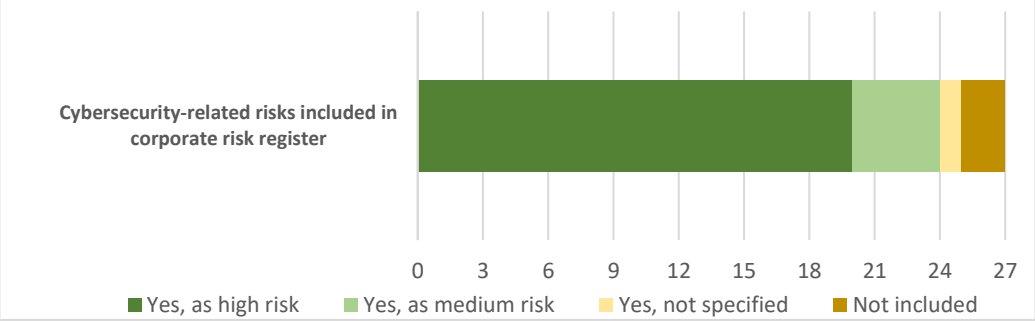
60. **Risk management paradigm already partially recognized.** The utility of applying a risk management lens to cybersecurity has already been recognized in various forums, although in practice the implications of viewing cybersecurity this way have yet to be fully understood and absorbed in many parts of the system. For example, the meeting records of recent symposiums of the Information Security Special Interest Group attended by cybersecurity experts included several agenda items touching on risk management, including a call on its members to engage with representatives from their respective organizations who served on the High-level Committee on Management Risk Management Forum in order to ensure that cybersecurity risks were included in the perspectives contributing to the Forum's risk maturity

[14] JIU/REP/2020/5.

model.[15] The need for including cybersecurity considerations as part of organizations' wider enterprise risk management and business continuity frameworks was also underscored by the audit and oversight committees of several organizations. In fact, most addressed cybersecurity as part of their mandate on corporate enterprise risk management and emphasized the need for greater integration between the ICT and risk management functions. Furthermore, state-of-the-art cybersecurity standards, including ISO 27001, the Control Objectives for Information and Related Technology and the United States National Institute of Standards and Technology framework, treat cybersecurity risks as business risks, far beyond the scope of the computing infrastructure, and stress the strategic dimension of improving organizations' cybersecurity posture, which is considered to be best achieved when correlated fully with corporate-level risk management.

61. **Attention to risk management in participating organizations.** The degree to which cybersecurity has been embraced as a risk management issue varies across the participating organizations surveyed by JIU. In their responses, the vast majority (24 out of 27) stated that cybersecurity-related risks were formally included in their corporate risk register. Of these, 20 confirmed that the level of risk assigned was "high" (figure V), and 19 had included specific cybersecurity risk mitigation measures in their corporate risk register. The Inspectors were provided with internal risk management documentation by only 11 participating organizations, which shared, in confidentiality, extracts of their risk registers. Given the incomplete data set, conclusions drawn must be regarded as preliminary. However, comparing some of the risk registry samples provided, certain differences in assessing, categorizing and planning for cybersecurity risks could be observed. On the one hand, some organizations placed the emphasis on strategic aspects, such as the potential impact of cybersecurity incidents on the reputation, productivity and finances of the organization. On the other end of the spectrum, there are examples of risk registries that are focused almost entirely on ICT security, with the primary emphasis being on preserving the availability of information rather than its confidentiality and integrity. The latter tend to require more complex measures than those geared towards avoidance of technical disruptions and "downtime" only, which may explain why these aspects have been tackled to a lesser degree in the documentation reviewed. One drawback of risk registries that place mainly technical aspects of cybersecurity at the centre of attention is that they may fail to establish the link between these elements and the broader consequences for the organization.

Figure V
Inclusion of cybersecurity in corporate risk registers, in number of participating organizations



Source: JIU questionnaire 2020.

62. **Mitigation measures require more attention.** One area that stood out, even with the limited data available to the Inspectors, was the level of articulation of cybersecurity risk mitigation measures, either as part of a risk management framework or outside of it. As pointed

[15] CEB/2019/HLCM/DTN/02.

out by audit and oversight committees, mitigation measures are often descriptive of the status quo (e.g. detailing the measures already in place, rather than envisaging actions in anticipation of specific risks in a proactive manner), resulting in a self-serving process of setting goals that have already been achieved in order to improve reporting, rather than an earnest effort to devise meaningful mitigating actions as yardsticks for gradual implementation. Conscious of the fact that some organizations may have deliberately chosen to present their mitigating measures in unspecific terms to protect the entity's defences, **the Inspectors are of the opinion that the emphasis in the future should be on formulating mitigating measures in a forward-looking manner that remains reflective of existing constraints and weaknesses, acknowledging the fact that this may involve additional effort to reach newly established targets as well as a transitional period of reporting that may show less than fully achieved goals.**

63. **Road maps.** In some organizations, cybersecurity risk assessments led to the adoption of a corporate road map to improve the cyberresilience of the organization, prepared by management with feedback from all relevant internal stakeholders and, in many cases, presented to the legislative or governing bodies for endorsement. The Inspectors found such road maps most meaningful when they were designed as a multi-year plan linked with milestones and indicators of achievement, accompanied by a shift in resource allocation to ensure that mitigation measures could be implemented in practice. Such road map development processes had been completed or were ongoing in several organizations at the time of drafting of the present report (ICAO, the Food and Agriculture Organization of the United Nations (FAO), the United Nations Population Fund (UNFPA), the Office of the United Nations High Commissioner for Refugees (UNHCR), the United Nations Office for Project Services (UNOPS) and the World Intellectual Property Organization (WIPO)) and were considered to be a good practice to streamline improvement efforts across the organization.

64. **Moving from awareness to proactive management of risks.** In conclusion, while many participating organizations have realized the importance of cybersecurity considerations and attempted to include them, to varying degrees of articulation, in their broader risk management frameworks, the overall system-wide picture is still uneven and requires further attention to move from mere awareness of cybersecurity risks to truly managing them according to the requirements of each entity, acknowledging that in this area zero risk is not attainable. **The Inspectors therefore concur with and echo the caution demanded by cybersecurity experts: the stakes are high, and a risk-based approach is called for (annex II).** The emphasis in future needs to be on developing effective and meaningful risk mitigation measures in conjunction with robust business continuity planning. Cybersecurity experts' contribution to and full involvement in internal risk management processes, from design to implementation and monitoring, will be crucial to achieve these objectives.

C. Building on the convergence between physical security and cybersecurity

65. **Blurred lines between physical security and cybersecurity.** The somewhat philosophical question of whether cybersecurity was predominantly to be considered a "cyber" – that is, a technology-driven – issue or a security issue (comparable to physical safety and security but transposed into the digital realm) emerged early on, even during the conceptualization stage of the present review, and sparked a rich debate among the stakeholders interviewed by the Inspectors. Even though the United Nations system organizations have traditionally treated physical safety and security and cybersecurity as separate domains, both are concerned with protecting the organizations' personnel and preserving their assets. To that end, both functions are in the business of managing uncertainty or risk by anticipating, protecting against and knowing what to do in the face of an attack, making risk management a common denominator connecting the two domains. Physical security and cybersecurity also share the understanding that even the best protection measures will not completely prevent attacks from breaking through an organization's defences, no matter how elaborate or sturdy they may be. Finally, when evoking scenarios that might illustrate where cybersecurity ends and physical

security begins or vice versa, it quickly became evident that the physical and digital realms may not be as readily separable as it may appear at first glance.

66. **Physical security and cybersecurity intersect in practice.** Currently, systems supporting the safety and security function that are operated without relying, in some form, on the use of ICT are rather the exception than the rule. As a result, the consequences of cybersecurity breaches affecting such systems are likely to materialize in the physical world, sometimes to the point of exposing people's lives or physical integrity to significant danger. There is no shortage of examples of the ways in which cyber and physical security intersect in practice. For example, hackers may take control of a security gate, exploit weaknesses in safety protocols to plant spyware on electronic devices or to download confidential information onto portable devices, gain online access to office floor plans with a view to studying the best target for an armed attack, or engage in virtual identity theft to lure others into situations where they end up endangering themselves unwittingly by relying on information from otherwise trusted sources fraudulently impersonated by cybercriminals. In addition, porous security measures compromising the protection of premises, data centres, server rooms or digital access points from unauthorized entry or other forms of undue interference emanating from physical hazards (natural or man-made) may have a direct adverse impact that is felt in the digital sphere. The convergence of the two worlds may be even more pronounced in field locations, which tend to be further removed from central cybersecurity control mechanisms and monitoring, while also being a potentially more attractive target given that the information held is directly critical for the safety of life and limb. An example of this would be data on the whereabouts or movement of personnel in less protected areas.

67. **Institutionalized links between physical security and cybersecurity remain sporadic.** Across the participating organizations, responses to the JIU questionnaires and subsequent interviews with officials revealed a varying degree of realization of the interlinkages between the physical realm and the cyberrealm. The corporate architecture of only two organizations reflects an actual integration of the physical safety and security and the cybersecurity management frameworks, either through the placement of the two functions in one department with a shared reporting line to a deputy-executive level position with an overall organizational security mandate (WIPO), or through the strategic articulation of both functions as two contributors among many to a broader "organizational resilience management framework" that combines defences against all types of threats, whether physical, digital, political, natural or other (ITU). Other organizations have recognized that there are convergence points and synergies to be gained and have formalized the coordination and exchange of information between the two functions to a degree, for example through dotted reporting lines, joint briefings to senior management or cross-participation in meetings, or by having both functions contribute on equal footing to corporate processes such as risk management or business continuity planning or on an ad hoc basis in emergency response situations requiring input from both. Also, collaboration on specific operational-level measures (e.g. consolidating information on cyber and physical threats for mission travel advisories or jointly devising sophisticated technological solutions for personnel identification and access cards for admission to premises) is already under way, with some tangible benefits for the security posture of the organizations concerned. Even in parts of the system where physical safety and security is considered distinct from and largely unconcerned with cyberspace, organizations have provided evidence of occasional, informal contacts between the two domains. Nevertheless, for the majority of organizations surveyed on this point, the reality remains that the link between physical security and cybersecurity is understated or only marginally acknowledged, which is also the case at the system-wide level (paras. 159–164).

68. **Upskilling cybersecurity capacity inside the physical safety and security function.** In the Inspectors' opinion, there is potential for building on the convergence between physical security and cybersecurity to the benefit of both domains and organizational resilience more broadly. One option would be to explore the possibility of building internal capacity by upskilling and expanding the profile of a critical number of safety and security professionals

and incorporating cybersecurity aspects into their future skill set, notably by rethinking the way current job descriptions are framed (e.g. augmenting them with elements of cyberthreat intelligence processing, threat modelling and similar analytical capabilities). The perception that cybersecurity is inherently unrelated to and dissociated from the duties of such professionals may partially be grounded in the long-standing practice of recruiting them primarily from among police and military forces – a notion that fails to recognize that the latter have themselves already developed modern capabilities in the required domains. The expertise exists, and it is readily available for United Nations system organizations to recruit from. Once built, this additional capacity would complement rather than replace the advanced and well-oiled machinery of the present traditional security-minded workforce and enable it to interface more effectively with a dedicated cybersecurity capacity within the respective United Nations system organizations. The Inspectors recognize that the two domains have distinct and highly specialized capabilities that are well-built to serve their respective protection objectives, and that, therefore, attempts to merge them into one structure or subsume one into the other would not appear prudent without further study. However, efforts to expand existing capacities to improve the linkages between the two domains may be one of the elements to explore, with a view to achieving a more holistic approach to the protection of organizational personnel and assets, as envisioned in recommendation 5.

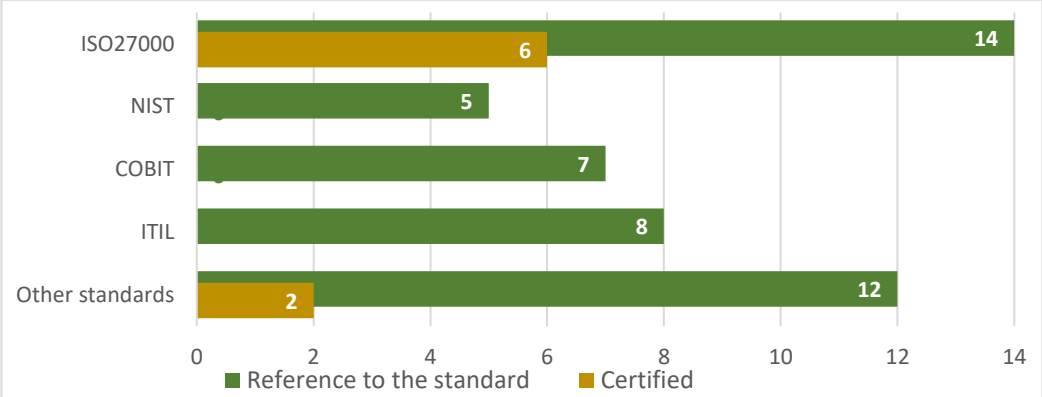
D. Shaping regulatory frameworks for compliance and accountability

Industry standards on information security

69. **Standards used by participating organizations.** Cybersecurity is a domain for which a number of national and international industry standards have been developed that provide guidance and benchmarks with a view to building resilient Information Security Management Systems. The term, coined by the International Organization for Standardization, refers to the totality of measures – managerial, regulatory and technological – that reflect an entity's approach to cybersecurity. It comprises a complex set of controls, ranging from rules and policy documents to management tools and processes, security concepts and risk management strategies, among others. Participating organizations referred to a wide range of such standards, sometimes more than one, which they indicated were selected on the basis of their relevance to each organization's specific setting and requirements and were further refined by recording those controls of a particular standard that were most relevant in a tailored "statement of applicability". The Inspectors recall that, already a decade ago in 2011, the Information and Communication Technologies Network endorsed pursuing the ISO 27001 standard for agencies of the United Nations system,[16] and in 2017, the Information Security Special Interest Group reaffirmed this position. The present review confirms that most United Nations system organizations are either already certified, planning to get certified under ISO 27001 or have chosen to voluntarily align their framework with it without seeking formal certification. Alongside ISO 27001, there are several other standards that are used by United Nations system organizations, which are reflected in figure VI below and further described in annex III. Only three organizations have not referenced any standards or have not communicated information in this regard.

[16] CEB/2011/HLCM/ICT/16.

Figure VI
Main industry standards used by JIU participating organizations



Source: JIU questionnaire (2020) and interviews.

Abbreviations: NIST, United States National Institute of Standards and Technology; COBIT, Control Objectives for Information and Related Technology; ITIL, Information Technology Infrastructure Library.

70. **Formal certification versus reference to standards.** Regarding the utility of formal certification as opposed to softer forms of voluntary compliance, the Inspectors found divergent views among the experts. Indeed, it is a management decision to seek certification as a means of providing reliable reassurance to legislative and governing bodies as well as to external partners based on the formality of the process and the statement of certification, as well as the rigour applied in requiring yearly independent audits to maintain it. It may also serve as a recurrent trigger for innovation, given the requirement to demonstrate constant enhancements. At the same time, some organizations argue that certification may be too costly and elaborate to justify the investment. They also criticize its heavy reliance on formal compliance, which may incentivize deliberately favourable rather than realistic reporting. The Inspectors acknowledge that certification and alignment can both be useful options, especially at different stages of a gradual build-up of cyberdefences. This is especially true because standards can be used in different ways, including as a benchmark or framework for auditing purposes, as an internal road map for self-improvement, as an additional incentive for compliance with controls or as an inspiration or a reference tool for tailored approaches.

71. **Benefits of reference to standards.** The Inspectors refrain from arguing for a particular industry standard or a harmonized, system-wide approach thereto, because different standards may validly serve different purposes and offer suitable choices for different levels of maturity. Accordingly, there is no one right standard, nor one correct approach to cybersecurity, but there is a strong case to be made for drawing inspiration – whether formally or informally – from relevant industry standards when setting up and managing one's own regulatory framework. Participating organizations must therefore identify the adequate standard, and within that, the most relevant controls based on the level of protection required to match their own situation, in accordance with the requirements and risks identified following proper organization-specific cybersecurity risk assessments. The Inspectors note, without judgment, that the corporate decision in this regard may also have implications at the system-wide level, where the use of the same framework or standard may lead to easier comparability and provide a common language among all. Conversely, a variety of approaches may, in the context of inter-agency mechanisms, provide additional opportunities for cross-organizational debate, the testing of assumptions, a more critical examination of one's own choices against those of others, and mutual learning more generally, which ultimately benefits the organizations individually.

Policy frameworks and procedures

72. **Prerogative to build appropriate regulatory framework rests with each entity.** Universally applicable, authoritative guidance on how to regulate cybersecurity matters is not readily available beyond the variety of industry standards mentioned above. The absence of an international legal instrument or framework in this sphere can be attributed to the fact that the domain itself is multifaceted and difficult to delineate, and as such represents a complex terrain for regulation, even in the context of the domestic law of any one State alone. Elevating this complexity to the international arena, it becomes even more difficult to define a common framework governing the relations between States as well as other public and private sector stakeholders operating in cyberspace. At this point in time, there is neither a legally binding instrument in international law nor a single normative framework for the United Nations system organizations that regulates cybersecurity specifically. As a consequence, the international governance framework of cyberspace can be best characterized as a patchwork of formal and informal institutions and norms composed of intersecting and overlapping technical standards, contracts, laws and intergovernmental decisions. In the absence of a consistent framework that could serve as a model, each entity retains the prerogative – within the confines of the parameters dictated by its constituent instrument and associated legislative and governing body decisions – to formulate its own rules in relative autonomy and choose what its blueprint for cybersecurity will be.

73. **Cybersecurity routinely referenced in ICT strategies.** The way in which cybersecurity is covered in existing regulatory frameworks, in other words, the normative setting within which organizational functions operate, varies and tends to reflect the historical evolution of cybersecurity as a domain that originated in the ICT sphere and grew into its own discipline from there. A few organizations articulate cybersecurity entirely independently of ICT, treating it as a stand-alone matter in its own right and on equal footing with physical security (WIPO) or as part of a broader vision of organizational resilience management (ITU), but such approaches remain the exception. Most participating organizations have elaborated a corporate multi-year strategic document that outlines their vision in the area of ICT, and, in their vast majority, these ICT strategies incorporate cybersecurity considerations. That being said, some contain only a basic reference, sometimes complemented by more elaborate lower-level guidance, while others include entire chapters dedicated to the subject. **Irrespective of the degree of elaboration of cybersecurity guidance within organizations' broader ICT strategies, the Inspectors considered the existence of references to the matter in such ICT strategies to be a positive first step.**

74. **Specific cybersecurity policies exist or are being developed in many participating organizations.** It is worth noting that the core documents of several leading industry standards require the existence of specific cybersecurity policies and documented procedures as a key pillar of the controls that underpin an entity's Information Security Management System.[17] The present review found that many organizations had produced such dedicated guidance, and that those who had not were, with few exceptions, in the process of developing it. More specifically, there was evidence of 17 organizations having put in place regulatory instruments specifically on cybersecurity (three of which are currently being revised), while 4 confirmed to be in the process of developing new policies. Only three organizations reported having neither formulated nor initiated the formulation of specific cybersecurity policies or regulations and stated that they relied on their ICT policies and procedures to address the issue. With few exceptions, organizations can therefore be said to have recognized the importance of having an

[17] ISO 27001, in its normative list of control objectives, starts with control A.5 "Information security policies", stating that a set of policies should be established and communicated to employees and relevant external parties. The United States National Institute of Standards and Technology, in its core document "Framework for Improving Critical Infrastructure Cybersecurity", as part of the governance category specifies that "the policies, procedures and processes" are to inform "the management of cybersecurity risks".

articulated framework of reference to guide their approach to cybersecurity. Annex IV lists the key instruments that govern cybersecurity within the regulatory framework of the participating organizations.

75. **Frameworks generally complex, heterogeneous and multilayered.** Regardless of whether more elaborated cybersecurity regulatory frameworks have been put in place or whether the organizations in question refer to those applicable to ICT more generally, the frameworks encountered by the Inspectors tended to be scattered across a set of strategic, policy, procedural and technical guidance documents. The terminology associated with such documents varies across participating organizations, ranging from strategies to mission statements, policies to administrative instructions, standard operating procedures to guidelines, and "playbooks" to protocols, and these often overlap conceptually or are even used interchangeably. The United Nations International Computing Centre has developed a model to represent the different normative components of an Information Security Management System as layers, reflecting the highest level of abstraction on top and the broadest level of detail at the bottom, and has supported several United Nations system organizations in assessing and improving their existing regulatory and governance frameworks. Building on that model, annex IV provides an overview of the objectives, formats and typical content encountered in the organizational cybersecurity and ICT documents reviewed by the Inspectors, acknowledging that a detailed qualitative content analysis across all participating organizations would exceed the scope of the present review.

76. **Contextual adaptation and periodic review.** Ensuring that policies are reflective of an organization's specificities may involve adjusting them to mirror the exact controls required by the industry standards an organization has chosen to follow, if applicable. An example of this was encountered at WFP and the United Nations Development Programme (UNDP), where, for each ISO 27001 technical control that the organization had selected to include in its "statement of applicability", there was a corresponding policy statement in its regulatory framework. It may also involve regulating areas of particular concern that may be more relevant to some organizations than to others, such as guidance on safe practices for in-house website, database or application development. The variety of policies and differences in the set-up of regulatory frameworks observed can thus be validly explained, at least in part, by their contextual adaptation to an organization's reality, rather than indicating the lack of a systematic approach to regulation. Furthermore, in the fast-evolving domain of cybersecurity, it is even more important for normative guidance to remain adaptable and relevant, which some organizations have sought to achieve by subjecting the guidance to periodic review. In this regard, it can be considered a good practice to insert into such guidance documents and policies explicit time frames by which they should be formally reviewed and revised as necessary, accompanied by indications about who is responsible for initiating such a process.

77. **Existence of guidance is important, irrespective of scope, degree of elaboration or organizational setting.** Given the significant variety of cybersecurity-related matters that can be subject to regulation, it is difficult to map, let alone prescribe, the precise types of policies or procedures that would optimally support a robust cybersecurity framework. Suffice it to say that the existence of even basic guidance in this often highly technical and multifaceted domain is important to ensure coherence and consistency in the application of security measures, irrespective of the size of the organization or the resources it has at its disposal.

Mainstreaming cybersecurity

78. **Mainstreaming.** It would be short-sighted to stop at only ICT and cybersecurity-specific policies when devising a regulatory framework for greater organizational cyberresilience. Maintaining the cyberdefences of an organization is the shared responsibility of many departments, and mainstreaming can go a long way towards achieving an organic rather than imposed adoption of a whole-of-organization approach (paras. 92–95). A number of organizations show signs of already having started mainstreaming cybersecurity considerations across their different policies. However, assessing the extent to which cybersecurity has been

mainstreamed into the overall regulatory frameworks of participating organizations would require a much broader scope of analysis and more in-depth study than the present review allows. The Inspectors suggest a few pointers for consideration in box 4.

Box 4: Pointers for mainstreaming cybersecurity across corporate regulatory frameworks

- Elements relevant to cybersecurity can be incorporated directly into the policies, processes and practices guiding the work of departments such as human resources, procurement, communications or the legal service. Two examples of the latter are including specific vetting requirements for the engagement of external service providers into the procurement manual, and inserting the steps to follow in managing cyberrisks throughout the project life cycle into the project document template or into programmatic guidance documents used by business units in their daily work.
- The roles and responsibilities of departments or functions other than those dealing directly with ICT or cybersecurity can be assigned and expressly reflected within the main regulatory instruments in place. For example, the corporate information technology security policy of WFP details the roles and responsibilities of different categories of individuals such as information owners, information custodians, information users, supervisors and personnel. WIPO is another example.
- Avenues can be set out through which all relevant stakeholders beyond ICT and cybersecurity staff are required to routinely contribute not only to the formulation of those instruments but also to their implementation (e.g. by including representatives of such stakeholders as members in relevant internal governance bodies or foreseeing a clearance process for policies that require certain stakeholders to be consulted before approval of the final text).

Source: Prepared by JIU.

Compliance and accountability

79. **Accessibility as a prerequisite of compliance.** The most well-articulated regulatory framework is only as effective as the degree to which the relevant parties comply with it. Compliance may be influenced by several factors, including the accessibility of materials that set out in clear terms what is required of each stakeholder and member of the workforce and why. This latter point was emphasized by one chief information security officer interviewed by the Inspectors, who pointed out that the issue was not so much the lack of written guidance but rather the poor understanding on the part of users as to why that guidance was in place, what it protected, and how the failure to be familiar with and apply it might impact both the individual and the organization. The importance of this awareness is further developed in other parts of the present report (paras. 97–103) and includes the need for simple, non-technical and engaging language and messaging that focuses on making the consequences of risky cyberbehaviour palpable for the individual. An example of a well-structured and comprehensive repository of cybersecurity guidance material, including plain language videos, posters, brief "how-to" articles, frequently asked questions, and the full set of applicable regulations and policies categorized by topic and complemented with explanatory notes, was found at the United Nations Secretariat, linked directly via one click from the main intranet page of the Office of Information and Communications Technology.

80. **Current response to cybersecurity non-compliance may be inadequate.** An important factor with a high probability of influencing compliance is the existence of effective enforcement measures that can be applied in the event of non-compliance, ideally reinforced by the knowledge and expectation that non-compliant behaviour will be sanctioned. Few policies

reviewed by the Inspectors contained specific language on sanctions for cybersecurity breaches. Even in cases where specific sanctions are mentioned in the relevant policies, information gathered regarding their implementation in practice suggests that they are rarely enforced, and, as a result, employees engaging in risky practices are not generally held accountable. In most participating organizations, it is the policy on acceptable use of ICT resources that may contain some specifics on sanctioning ICT-related misconduct, which generally includes cybersecurity breaches. Generally, such breaches are subjected to the same type of disciplinary action as that attached to violations of any other staff rule or regulation. However, the standard processes are, even when successfully invoked and completed, known to be slow, cumbersome and resource-intensive and tend to be triggered only in particularly egregious cases of ICT-related misconduct.

81. **Need to consider a more nuanced sanction system.** In the case of cybersecurity breaches, which are often due to simple ignorance or carelessness, **the Inspectors are of the view that more easily deployable, less formal and invasive sanctions may represent a more promising approach.** Such sanctions would address the problem in a more direct and immediate way that is commensurate with the severity of the infraction. However, a balance needs to be struck to ensure that the consequences of non-compliant behaviour are still sufficiently felt by the committing parties in order to encourage better cyberhygiene and more responsible conduct. Implicit recognition of this fact can be detected in the practice of some organizations, which distinguish between minor and more severe violations in their relevant cybersecurity policies. However, it was less evident whether they had succeeded in translating this distinction into sanctions that were more adapted to minor infractions while still being effective. For example, some policies foresee informing line managers or the head of the ICT department, which may represent the only "soft" pressure for compliance available but does not suggest any consequence other than potential embarrassment. A counter-example worth noting, due to its specificity and direct adverse effect on the user without being excessively punitive, is provided by IAEA, which includes in its policy an explicit, non-disciplinary sanction in the form of revoking non-compliant individuals' right of access to information systems. It is further noteworthy that the policy recognizes the need for proportionality in requiring awareness before one can be sanctioned for wrongdoing and balances the objective of effectively protecting organizational assets against ensuring that enforcement action does not imply policing the workforce. In practice, the revocation is implemented on a temporary basis and after repeated warnings. The Inspectors would like to stress that any meaningful sanction mechanism cannot be implemented without explicit support from the executive head, which is a contributing factor in the success of the cited example. **In the Inspectors' opinion, the executive heads should also explore the possibility of introducing incentives for reporting incidents and encouraging individuals to take responsibility for their unsafe or risky practices.** In doing so, it will be important to find ways of reconciling the objective of deterrence through more nuanced sanctions with that of incentivizing reporting without fear of repercussions.

E. Harnessing the contributions of oversight mechanisms

82. **Audit and oversight at all levels attentive to cybersecurity.** The Inspectors examined how oversight bodies had dealt with cybersecurity considerations in the context of their respective areas of focus, whether at the level of the internal audit function (aimed primarily at assessing compliance with policies and procedures), at the level of external audits (concerned mainly with financial and compliance auditing, and on occasion performance auditing in administrative and managerial areas) or at the level of audit and oversight committees (chiefly advising on broader organizational issues for priority attention and action by senior management as well as legislative and governing bodies). The Inspectors welcome the fact that, at each of these levels, cybersecurity has featured as a subject of interest over the last five years, and in some organizations for even longer than that.

Oversight bodies seized with cybersecurity matters

83. **Internal and external audit mainly focusing on ICT, including cybersecurity to an extent.** ICT-related issues are generally well-integrated into risk-based internal audit planning. However, during its research JIU found only a limited number of audit assignments focusing specifically on cybersecurity during the last five years. In terms of capacity to conduct such assignments, only a few organizations maintain in-house ICT audit expertise, while the majority rely on experts hired externally. This approach appears to be satisfactory in most cases. ICT has also been an area of focus for external auditors in many participating organizations over the years, who have addressed topics such as business continuity, risk assessment and risk management, ICT policies, and ICT assets management. Overall, the management responses consulted by the Inspectors showed an acceptance of the resulting recommendations and indicated the measures taken towards implementation.

84. **Audit and oversight committees paying sustained attention to cybersecurity**. In 2016, the representatives of oversight committees of 19 United Nations system entities "identified, inter alia, the risks associated with cybersecurity in a digitalized environment as an area of focus and agreed to challenge management on its understanding and readiness."[18] Indeed, the content analysis of the reports of these committees shows that there has been sustained attention focusing on strengthening the governance and risk management aspects of cybersecurity, even though none of them include a specific reference to cybersecurity in their terms of reference, and only four include a reference to ICT. The committees mostly addressed such issues as part of their mandate on corporate enterprise risk management or, where applicable, when following up on the implementation status of ICT-related internal or external audit recommendations. The present review showed that specialized expertise was not systematically present within the membership of the audit and oversight committees, as only four committees appeared to benefit from such expertise, while most relied on external advice on an ad hoc basis, similarly to the prevailing arrangement for the internal audit function. It is commendable that these committees embrace the topic, not only because doing so may support management in pursuing a risk-based approach to cybersecurity but also as a way of informing legislative and governing bodies about relevant cybersecurity risks, thereby enabling them to contribute to organizational risk mitigation.

Value of oversight recommendations for enhancing organizations' cybersecurity posture

85. **Oversight recommendations driving positive structural changes.** Participating organizations reported that significant structural changes in their approach to cybersecurity had originated from observations made by oversight bodies, thus highlighting the added value of such mechanisms. During interviews, officials responsible for ICT and cybersecurity generally valued oversight reports as drivers of change, raising awareness among senior management of the need for greater attention to a robust cybersecurity posture. The Inspectors indeed found examples where internal audit recommendations directly contributed to the enhancement of cybersecurity within the organization concerned, such as at WIPO. Other examples were found at ICAO and UNFPA, where an audit recommendation led to the elaboration of a multi-year road map; at UNESCO, where a chief information security officer position was created; or at the United Nations Secretariat, where compliance with information security training was significantly enhanced. External auditors also formulated recommendations on cybersecurity-related matters for 16 participating organizations in the last five years, notably regarding compliance with information security training, data recovery, users' access control and resources to be dedicated to cybersecurity. The utility of audit recommendations appeared to be better recognized when going beyond a compliance approach to operational and technical aspects and instead proposing strategic improvements, acknowledging that mere compliance with regulatory frameworks did not equal protection. At the same time, many organizations

[18] See A/72/295, paras. 40–43.

have expressed concern regarding the fact that such recommendations had on occasion not taken sufficient cognizance of resource constraints and operational realities, which rendered some of them less likely to be implemented.

86. **Cybersecurity expertise to inform oversight function in a systematic fashion.** To ensure that oversight bodies provide maximum value from a cybersecurity point of view, it is important that they have access to and understand well all relevant information relating to related risks, capacities and constraints within an organization. The most effective way of doing this is by ensuring that the knowledge and experience of the cybersecurity experts within an organization can inform and feed into the work of the oversight function. A variety of options exist in this regard, some of which have already taken root in the practice or even the regulatory frameworks of participating organizations, either individually or in combination, and can be considered as good practices. These include the following: (a) the chief information security officer or the relevant unit is mandatorily consulted for risk-based audit planning, and fully involved in determining relevant controls and indicators; (b) cybersecurity information is communicated to oversight bodies according to the needs of their respective mandate, be it through the reporting of incident metrics, ad hoc or regular briefings, or through other means; (c) any audit report or recommendation touching on cybersecurity is shared for comment with the chief information security officer or unit before finalization to alleviate concern about recommendations not being sufficiently grounded in organizational realities and thus becoming unimplementable.

F. Instilling a cybersecurity culture from the leadership down

87. **Leadership needs to encourage acknowledgment of mistakes and vulnerabilities.** As discussed above, the cybersecurity posture of an organization is also a matter of a strong internal culture, which starts with the attention and priority given to the issue by executive management – the tone at the top. However, it does not stop there and needs to cascade down to every single member of the workforce. To this end, a continued commitment and engagement of the top echelons of an organization is needed and must go beyond mere statements profiling cybersecurity as a corporate priority. A key element would be to encourage an internal culture in which acknowledging the occurrence of incidents is not seen as a failure but rather as a starting point for addressing a shared problem and for better protecting the organization and its assets by demonstrating joint and individual ownership and accountability for mistakes and weaknesses. In this regard, something can be learned from the law enforcement culture of the physical safety and security domain, where the occurrence of incidents is taken for granted, and the expectation is that they will be reported and dealt with as a matter of course, without judgment. **The Inspectors consider it the responsibility of the executive head to instil such a culture in all functions and all locations where the organization is present, since information systems are interconnected and interdependent, and an attack or intrusion anywhere could lead to a compromise everywhere**.

88. **Executive management awareness and accountability as a starting point.** The first step towards instilling a new mindset and culture is for senior leadership itself to be aware of the risks associated with cybersecurity and to develop an understanding of the implications of inaction and poor cyberhygiene by taking a greater interest in the issue. This can be achieved by requesting regular briefings from relevant officials inside the organizations, such as cybersecurity experts, risk management officers and representatives of oversight bodies, as well as through training and awareness-raising initiatives specifically targeting senior managers. Since 2020, in the United Nations Secretariat, the compacts concluded between the Secretary-General and senior officials contain provisions designed to foster awareness and accountability in this area. The consistency and effectiveness of the compacts and the performance indicators contained therein exceed the scope of the present review, but anchoring cybersecurity objectives in the performance appraisals of senior managers is a welcome step towards improving accountability and setting the right tone at the top. Moreover, initiatives such as the

presentation made in the context of the High-level Committee on Management to alert senior management to the continued impact of cybersecurity risks on operations, not only in terms of the disruption of administrative systems, networks and infrastructure, but also by jeopardizing substantive mandate delivery, should be encouraged, including within each participating organization.[19]

89. **Money alone does not buy a cybersecurity culture.** There are many ways in which executive management can inspire action and influence mindsets down the chain of command in concrete terms. For one, the importance accorded to cybersecurity can be expressed through an adequate allocation of resources. At the same time, money alone cannot solve the problem of cybersecurity preparedness, nor does it buy a culture of cybersecurity. Specifically, financial support does not relieve executive management of its responsibility to provide engaged leadership on cybersecurity matters, as reinforced in a recent report of the well-known cybersecurity think tank Gartner.[20] Expressions of support solely in financial terms may in fact shift the responsibility of executive management to the next lower level, where spending may occur without an overarching strategic vision. Resource allocation and related investments must be decided in a business context rather than from a purely technological or risk management standpoint, and executive management is best placed to make an informed decision weighing all considerations appropriately (paras. 108–109).

90. **Non-monetary ways of showing executive-level support.** Some good practices from participating organizations on meaningful, non-monetary support from senior management include the following actions taken by executive heads: visibly participating in awareness-raising programmes such as by recording video statements of support; addressing staff about cybersecurity matters in townhall meetings; sharing personal experiences with cybersecurity attacks with staff; publicly role modelling recommended behaviours; supporting frequent and regular simulated phishing campaigns for all levels of staff, including senior managers; ensuring responsibility cascades down by exerting pressure on senior managers to participate in training themselves and to hold their teams accountable for complying with policies and exhibiting adequate behaviours; and supporting the enforcement of proportionate sanctions, especially for "repeat offenders" who continue to violate cybersecurity rules and procedures. As stated above, acknowledging that mistakes happen and learning from them as well as tackling their consequences jointly as an organization is the starting point.

91. **Shift in mindsets requires time, consistent messaging and high-level support.** To take root in the attitudes of staff at all levels and thereby form a corporate cybersecurity culture, such measures will have to be repeated and will take time to show results. Experience shows that the chances of success are both increased and accelerated when a consistent message that cybersecurity matters and is not a one-off endeavour comes from the top of the organization. As stated at the eighth symposium of the Information Security Special Interest Group in 2019, "changing human behaviour is hard to do and requires repeated and consistent exposure to messages with new information and periodic re-learning, as well as an understanding of the latent risks technology presents and the consequences of bad computing behaviour".[21]

G. Implementing a whole-of-organization approach

92. **The role of administrative departments.** In line with the growing understanding that responsibility for cybersecurity cannot rest with ICT departments alone, the majority of participating organizations have recognized, in one way or another, that administrative as well as substantive departments have a role to play. In most organizations, this understanding appeared to be more pronounced in the responses to the JIU questionnaires with respect to administrative departments. As a matter of fact, whether formally reflected in organizations'

[19] See CEB/2017/HLCM/ICT/9.
[20] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.
[21] CEB/2019/HLCM/DTN/02.

regulatory frameworks or not, a series of administrative departments routinely contribute to the maintenance of organizations' overall cybersecurity protections. This includes: human resources departments facilitating cybersecurity training programmes; procurement services handling vendor relationships with external service providers, including their vetting from a cybersecurity point of view; legal services providing advice on regulatory, contractual or compliance issues; and communication departments managing public relations aspects with external stakeholders. Beyond their function-specific contributions, most of these departments are naturally expected to be predisposed to incorporating cybersecurity considerations in their daily activities, given that their core business involves handling sensitive information, including personal and financial data. Whether this happens to a sufficient degree in practice and can be considered to reflect an actual understanding by such departments of their privileged role as custodians of sensitive information is not evident from the materials studied by JIU. This may be an area deserving increased attention by heads of such departments and internal auditors and, where applicable, could be incorporated into cybersecurity assessments performed by external providers.

93. **The role of substantive departments.** In contrast to administrative departments, the information gathered during the preparation of the present review suggests that, with the exception of those participating organizations whose mandates impose a strict data confidentiality requirement as a core aspect of their work, cybersecurity is often seen by substantive managers as an administrative burden and operational constraint. Reportedly, programme offices were not receptive enough to the necessity of including cybersecurity and resilience requirements in the design and implementation of their projects and activities. In the words of a chief information security officer interviewed, "cybersecurity policies and procedures are often regarded as an impediment to speed of delivery rather than as protective shields for the reputation and assets of the organizations as well as for the efficiency of their operations." Against this backdrop, it is particularly important that executive heads actively counteract perceptions that enhanced cybersecurity measures impede operational agility or obstruct the attainment of mandated objectives.

94. **Mainstreaming and ownership of roles and responsibilities as the key to a whole-of-organization approach.** As stated above (para. 78), mainstreaming of cybersecurity considerations into the policies governing the work of respective departments and their practices would in itself be an acknowledgement that each function in an organization has a contribution to make towards achieving a whole-of-organization approach. In the light of the recent trend observed in many organizations towards decentralization and delegation of authority further down to mid-level managers, mainstreaming would also contribute to ensuring more direct organization-wide ownership and accountability by spelling out related responsibilities where they would be more readily consulted by each stakeholder in their respective role. Rendering the cybersecurity dimensions of programmatic and administrative functions more explicit through mainstreaming can reduce misunderstandings and a lack of ownership. For example, the Inspectors observed some tension between cybersecurity experts and representatives of other organizational units resulting from their respective perceptions of their own roles in ensuring a strong cybersecurity posture. **In this context, the Inspectors stress that, specifically, substantive departments need to take greater ownership of the cybersecurity dimension of their work.** However, the involvement of business units should not imply transferring responsibility exclusively to them as risk owners. Nor can cybersecurity experts be held solely accountable for protecting organizational assets without business units sharing a significant part of the burden. Striking the right balance will be important, and the mainstreaming of cybersecurity considerations across organizational domains can lay the groundwork for setting right mutual expectations between different departments and their respective roles in this regard.

95. **Role-based training should be further expanded.** One encouraging practice encountered across several participating organizations was the availability of role-based cybersecurity training opportunities and awareness-raising measures, which should be further

expanded to equip all stakeholders optimally for their respective contribution to organizational cyberresilience that they are expected to make. At the system-wide level, the Information and Communication Technologies Network has already encouraged targeting specific user groups based on their functional responsibilities, such as enterprise resource planning officers, finance and accounting specialists, procurement officers and executive managers. Some organizations have also developed tailored sessions for staff with sensitive missions or for field-deployed staff facing certain location or infrastructure-specific risks. Among these special audiences, executive and senior managers on the one hand, and programme managers on the other hand, may be worth prioritizing, as their own understanding of and attitude towards cybersecurity is likely to cascade down within their respective organization or unit and to impact the emergence – or not – of a cybersecurity culture in significant ways.

H. Establishing the workforce as a first line of defence

96. **The "human factor" – threat, defence and pillar of cybersecurity culture and resilience.** The majority of United Nations system organizations have put in place significant technological and operational measures to help prevent and mitigate the risk of cyberattacks (para. 38). However, there is consensus among the cybersecurity expert community that the challenge of educating every member of the workforce on his or her role in protecting the information and digital assets of the organization, as well as the importance of adhering to cybersecurity policies, procedures and best practices, persists. In many ways, the "human factor" has gained in importance in the global cybersecurity threat landscape, as reflected in the growing concern among participating organizations over individual end users being increasingly targeted through social engineering techniques (paras. 26–27). It has also proven to be particularly difficult to manage as a source of risk. Apart from being both the first line of defence and the weakest link in the digital safety net of his or her organization, every single member of the workforce also represents an important pillar of organizational cybersecurity culture and resilience. The adverse consequences of poor cyberpractices are manifold and often manifest as significant internal threats. These may be brought about by: errors committed by inattentive or unengaged users; a lack of awareness or alertness (often exploited in phishing attacks); poor data protection practices, such as the selection of weak passwords or the sharing of access credentials among several users; the use of unauthorized or outdated software; the development of applications outside of organizationally managed ICT environments; and unpatched or negligently maintained systems. Such behaviours are probably the most consistently pervasive forms of threats encountered by organizations on a day-to-day basis. It is therefore evident that empowering users to play an active role in improving organizational cyberresilience is imperative.

97. **Digital literacy is the non-negotiable starting point.** As a precondition for developing an understanding of how one's own cybersecurity practice affects the organization, the basic digital literacy of each member of the workforce is a non-negotiable starting point. Being able to operate in the digital environment is no longer optional for any person affiliated in whatever way with the United Nations and its work in the twenty-first century. Comfortable navigation of standard electronic equipment and applications must be a given for any and every user of the organizations' digital infrastructure, be it staff, affiliated personnel, experts on mission, conference delegates or any other person linking up with or tapping into internal cyberresources. Only after this fundamental requirement is met can one proceed to remind employees that preserving the confidentiality, integrity and availability of corporate information and assets is an integral part of everyone's job and responsibilities. The more challenging leap, however, may be that of evolving from raising awareness of cybersecurity rules, responsibilities and tools and guidance on healthy cyberpractices to achieving a sustainable behavioural change and a shift in individual and collective attitudes.

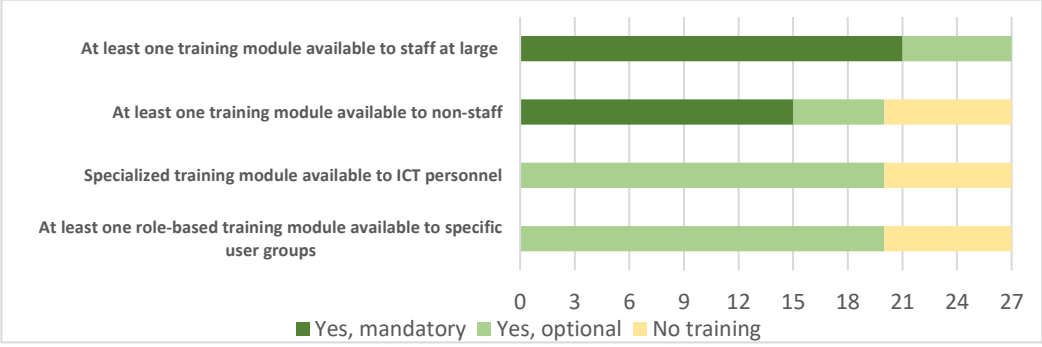
98. **Importance of training acknowledged.** One of the avenues by which to instil a shift in mindsets towards the recognition of cyberrisks and the development of a healthy cybersecurity

attitude is through strong training and awareness-raising programmes. This point has been stressed in professional literature and in the reports of audit and oversight committees addressed to the executive management of several United Nations system organizations. There is a certain paradox; extensive and layered technical protection mechanisms for infrastructure and systems are often in place, yet the ability of all members of the workforce to demonstrate practitioner-level knowledge of their use and capabilities appears to be lagging behind, at least in some organizations, according to the officials interviewed. The more robust the system is, the more the risk shifts towards the users, and among them those users with poor cyberhygiene represent the biggest risk. As stated by the Independent Audit and Advisory Committee for the United Nations Secretariat, the "lack of awareness could lead to compromises of information and communications technology systems, confidentiality and integrity of information".[22]

99. **Mapping of training opportunities for staff shows encouraging situation.** The importance of information security awareness training for the United Nations community has been stated by the Information and Communication Technologies Network over the years, and participating organizations have made efforts to beef up their offer in this regard.[23] Figure VII represents the information collected concerning four categories of target audiences, confirming the existence of mandatory training sessions for staff members in a majority of the organizations, but also shows that in some organizations such sessions remain optional. The content of such training usually focuses on the proper use of email accounts for business versus personal matters, the risks of opening attachments from unknown sources, guidance on password selection and handling, or safe behaviours when accessing external websites. In recent years, audit and oversight committees have alerted participating organizations to the need for enhancing the compliance rate for mandatory training courses, which is a welcome development in principle. However, the Inspectors wish to underline that compliance with mandatory training alone is rarely a meaningful indicator of awareness, nor does it provide sufficient assurance regarding the attainment of actual behavioural change. A more relevant indicator, although one that is likely to be more complex to track and analyse, might be to compare the number of users engaging in discouraged behaviours (e.g. clicking on a link or attachment in a phishing email) over time, particularly before and after training or awareness-raising interventions have been launched. Some good practices observed in relation to mandatory training include imposing a completion date for personnel newly joining the workforce in order to limit the time window for increased risks owing to unawareness, as well as requiring personnel to take refresher sessions on an annual basis to sustain the learning effect over time.

Figure VII

Information security awareness training in 2020, by training module and number of Joint Inspection Unit participating organizations



Source: JIU questionnaire 2020.

[22] A/73/304, para. 51.

[23] See, for example, CEB/2011/3 and CEB/2018/HLCM/ICT/10.

100. **Special attention to other categories of personnel and occasional users needed.** About half of the participating organizations also made information security training mandatory for other categories of their personnel, while the other half offered such training as an optional module or simply did not provide such opportunities. Attention to non-staff categories is indeed crucial. Members of such categories are often forced by resource constraints to use their personal devices to log on to corporate infrastructure. Moreover, infrequent users of corporate systems and infrastructure are less likely to be conversant in their correct and safe use in accordance with applicable organizational policies and practices. The lack of effective enforcement mechanisms for persons not in the direct employ and therefore outside the purview of the organizations' full disciplinary jurisdiction may further disincentivize and exacerbate already weak compliance. These challenges may be further accentuated in organizations where the composition of the workforce is heavily reliant on consultants, contractors and short-term personnel. **The Inspectors recall that training and awareness-raising initiatives need to encompass the entire workforce. Threats do not discriminate between different types of users. The Inspectors therefore suggest that executive heads of those organizations that have not made these modules mandatory take appropriate action.**

101. **Challenges regarding training.** A series of challenges faced by participating organizations that may affect the implementation of an effective cybersecurity training programme were communicated to the Inspectors. Several organizations pointed to financial constraints limiting their ability to develop or provide access to training opportunities, and, worryingly, some of them were forced to select certain categories of users to be trained over others. Financial aspects are further accentuated by the fast-evolving nature of the subject matter, which can quickly render course content outdated, requiring updates and expansions, often at significant cost. Another challenge lies in users' training fatigue, which may affect the effectiveness of the programme. High turnover in the workforce and the lack of authority over certain categories of personnel add additional layers of complexity. Field-deployed entities may face their own set of difficulties, much like for any other learning opportunities. However, this dimension could not be fully explored in the context of the present review. Lastly, cybersecurity officers pointed out the general lack of enforcement in the event of non-compliance with training requirements and correlated the possible ineffectiveness of many training programmes with the absence of sanctions, rendering even mandatory training de facto optional. **To ensure better enforcement, the Inspectors suggest that executive heads consider instituting a formal link between the completion of information security training and other corporate clearance procedures.** This may involve tying security clearance for field deployment and the granting or extension of ICT system access rights to evidence of training, including "refresher" courses, having been completed. A precedent for this approach already exists in the sphere of physical safety considerations before duty travel, where clearance to undertake such travel is contingent on the completion of basic field security training, without which approval to proceed will be refused.

102. **Awareness initiatives across the United Nations system.** There are multiple cyberawareness initiatives in the United Nations system about cybersecurity risks and recommended measures. An example is the October week on information security, an initiative joined by several organizations around the globe that features interactive sessions, games and information sessions. International Labour Organization (ILO) and WIPO programmes have been referred to as particularly innovative and effective, some having been recognized as such in the context of external audits. Additional ideas worth pursuing include focusing awareness-raising sessions on cyberrisks affecting the private sphere (e.g. risks faced by children or family pictures taken for ransom) in the hope that this would attract more interest and that the lessons learned would naturally spill over into the professional sphere at work. Some organizations organize in-person briefings by the chief information security officer for new staff, while others reinforce lessons learned by distributing brief video messages to staff who have fallen victim to a cyberattack. Simulated phishing campaigns are among the most popular means of awareness-raising and reportedly produce results (box 5).

Box 5: Simulated phishing campaigns produce results

Phishing refers to sending fraudulent emails alleging to be from a reputable source in order to induce individuals to reveal sensitive information. The attackers then use such information to obtain unauthorized access to the organization's systems, so as to scam the organization for financial gain or for other disruptive motives.

Simulated phishing campaigns simulate real life hackers' strategies and help to identify users who are more susceptible to being deceived into clicking malicious links or opening infected attachments. These simulations are also used to test the skills acquired through training. To be most effective, they should be accompanied by user-oriented services such as a clear point of contact and simple, widely known procedures for personnel to report suspicious messages. For example, some participating organizations have included a mechanism for reporting phishing messages by clicking a button directly in the electronic messaging application used by employees.

The figures shared with the Inspectors demonstrate the utility of such simulated phishing campaigns, since information security officers generally observed a reduction in the percentage of users opening suspicious messages and attachments as a result of successive campaigns. For context, the commonly acceptable share of internal non-complying users among the wider user community was around five per cent of the workforce, according to some cybersecurity officers.

Simulated phishing campaigns are frequently carried out as one component of more comprehensive penetration testing efforts. Often abbreviated as "pen" testing, such efforts consist of a series of hands-on exercises targeting an organization's network, systems and human resources to identify vulnerabilities, measure levels of compliance with policies and procedures, and assess the effectiveness of defences and recovery procedures.

103. **Moving from training modules to a consistent awareness-raising programme.** Rather than continuing to offer individual modules to everyone without being guided by a strategic vision, **the Inspectors advise organizations to aim to develop a comprehensive training and awareness-raising programme with clear objectives defined for each category of stakeholder, in accordance with the risks they may represent for the organization.** By following such a model, organizations would be in a position to move away from targeting completion rates as an indicator of compliance and instead use training as a proactive tool for changing the internal cybersecurity culture. Ideally, the programme should be implemented using innovative methods of delivery combining multiple approaches and messaging adapted to each audience. To increase the sense of ownership and facilitate better uptake of learning in this area, organizations may further wish to consider putting in place a peer support system and identifying individuals in all departments who could be trained as a resource in the implementation of the programme, providing hands-on assistance to other members of the workforce when and where needed.

I. Optimizing financial resource allocation for cybersecurity

Estimating the current level of resources dedicated to cybersecurity

104. **Cybersecurity resources available inside the United Nations system generally lower than outside, but difficult to quantify.** It is almost commonplace to say that United Nations system organizations have fewer resources at their disposal to allocate to ICT in general and to cybersecurity in particular, compared with entities of comparable size in both the public and private sectors. However, it is difficult to quantify the gap in both absolute and relative terms. For example, it was estimated that "less than one per cent of United Nations spend is on ICT,

and less than one per cent of that is reserved for information security, compared to an industrial average of around seven per cent".[24] In an effort to provide an evidence-based snapshot of the situation, JIU surveyed its participating organizations on the question of resource allocation to both ICT and cybersecurity. Perhaps unsurprisingly, the Inspectors arrived at the same conclusion as that indicated in the meeting records of the 2018 Information Security Special Interest Group symposium, namely that figures remained elusive for the system as a whole.

105. **Complexity and utility of estimating cybersecurity spending.** Several factors make it challenging to determine the resources available for cybersecurity. Cybersecurity costs (box 6) are generally not tracked as a separate budget line or category of expenditure. Cybersecurity-related funding may be subsumed under one or several budget lines (e.g. operational costs, personnel costs, or infrastructure or equipment costs) or thematic areas (e.g. within the ICT envelope or outside of it). The difficulty of locating information on cybersecurity resources and spending levels across budgetary documents and financial statements is further exacerbated by the diversity in budgetary structures, as reflected in the coexistence of regular budgets and voluntary (extrabudgetary) contributions, some of which may include stand-alone capital investment funds used for large-scale organizational infrastructure projects. Several organizations also distinguish (one-off) investment costs and (recurrent) operational costs, adding further nuance to the picture. In one organization, a large portion of ICT resources were even found to be federated across the programme budgets of business units maintaining ICT capabilities. Against this backdrop, making any reliable statement about the total resources available for cybersecurity is close to impossible. In any event, doing so is disproportionately complex compared to its utility: the level of resources allocated to cybersecurity in an organization bears limited indicative value regarding the level of protection offered.

Box 6: Cybersecurity costs

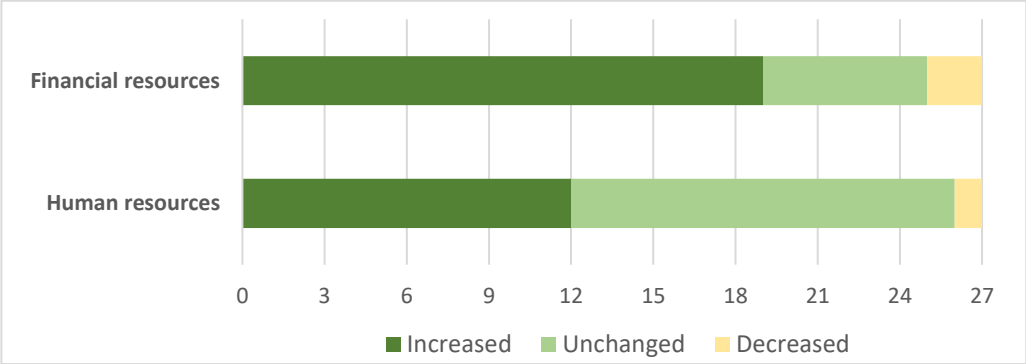
- **Direct costs.** The obvious (direct) costs of cybersecurity range from personnel expenditures (staff and contractors) and infrastructure-related expenses like hardware and software purchases (investment and maintenance costs and license fees) to services (e.g. threat intelligence subscriptions and outsourced services from commercial providers or the United Nations International Computing Centre). The proportional distribution of such costs varies and reflects each organization's choice in balancing in-house capacity versus outsourcing.
- **Indirect costs.** In addition, there are other (indirect) costs to factor in when putting a price tag on cybersecurity. In fact, significant financial impact tends to be associated with the measures taken for damage control in the wake of an incident, which includes mobilizing ad hoc capacities to reinstate disrupted services, patching newly revealed vulnerabilities, losing productivity while systems are down, training staff to better prevent and respond to intrusions and keeping existing specialized capacities (both human and technological) current.

106. **Recent trend: funding increased, but capacity constraints remain.** The Inspectors note that most participating organizations indicated an increase in the resources allocated to cybersecurity in recent years (figure VIII). At first glance, this may appear to be a promising trend. However, as evident from the graph, the reported increase of financial resources does not appear to have automatically translated into increased human resources capacity. In fact, the vast majority of participating organizations warned that the current level of resources available still constituted an obstacle to building an effective cybersecurity framework, with one organization even stating that the costs to secure and protect it against mounting cyberthreats

[24] CEB/2018/HLCM/ICT/4.

had tripled during the past two biennia. In the organizations' own assessments, resource constraints were found to have most severely impacted the human resource capacity and the availability of in-house expertise, the ability to make appropriate ICT infrastructure investments, and the ability to replace obsolete applications. In addition, in those organizations that operate amid severe resource constraints or within zero-growth budgets, resources newly allocated to cybersecurity may be the result of an internal re-deployment, possibly at the expense of other, mostly but not only ICT, investments. As this may prove unsustainable in the long run, the Inspectors are concerned that the resources available, even in cases where they increased, may not have grown at the same pace as the technological sophistication of attackers and the pervasiveness of ICT in the work of United Nations system organizations. As aptly stated in the context of the Information Security Special Interest Group, the increasing dependence on cyberenabled services has not been offset by an increased resourcing of the information security function.[25]

Figure VIII
Evolution of resources for cybersecurity as reported by JIU participating organizations (2015–2020)



Source: JIU questionnaire 2020.

107. **Sources of funding.** According to the information collected, resources for cybersecurity in most participating organizations are primarily derived from their regular budget. A number of them rely on a mix of regular and extrabudgetary resources, while very few rely exclusively on the latter. The relative predictability of regular budget resources may contribute to the sustainability of cybersecurity capacities, but this approach requires strategic planning to ensure that the required resources become available at the time they are needed. At the same time, extrabudgetary resources may allow for greater flexibility and may be more attractive for donors wishing to earmark such resources for cybersecurity. A handful of organizations maintain a special fund, either one dedicated to ICT infrastructure (WHO) or one that can be mobilized for major corporate projects (WIPO and IAEA). As alluded to in the context of longer-term road maps for the improvement of organizations' cybersecurity framework, investments in this area tend to have a multi-year dimension by nature. Current budgetary cycles may thus be too short to allow long-term strategic considerations to take root, yet not nimble enough to rapidly deploy funds to address ad hoc, short-term requirements that may emerge in a technological domain and threat landscape as fast-paced as that of cybersecurity. Special funds can fill a gap in this regard, provided that their governance principles and their terms and conditions, as agreed by legislative and governing bodies, enable them to do so.

[25] Ibid.

Towards optimization of cybersecurity investments

108. **Business case needed to substantiate resource requests to governing bodies.** It is evident that organizations cannot expect their resource allocation requests to governing bodies to be successful in the absence of proper justification for the prioritization of cybersecurity investments over other organizational spending. **As a starting point, the Inspectors recommend anchoring resource requests in a thorough risk assessment and in a business case detailing the costs, benefits, risks and expected savings and referencing the potential financial implications of not making the investment.** Such an approach is most effective when coupled with a proposed implementation plan and schedule, for example in the form of a road map, as argued elsewhere in the present report, and when reporting on progress is conducted on a regular basis. The Inspectors observed that, when executive management submitted a convincing business case stating a clear objective and parameters for improvement and demonstrated the criticality of the investment, governing bodies were generally more prepared to support the endeavour with dedicated resource allocations. This has been the case in recent years at ICAO, ILO, UNHCR, WIPO and other organizations and is an encouraging practice, as it is likely that the growing sophistication of cybersecurity threats will continue to require more resources, not fewer.

109. **Cybersecurity expenditure can and should be rightsized.** It goes without saying that a strong, well-protected cybersecurity framework comes at a price, and, if United Nations system organizations are serious about protecting their information, systems and digital assets, they must appropriately resource their cybersecurity frameworks. Attempts to determine the appropriate level of cybersecurity-related resources as a percentage of corporate ICT budgets did not yield meaningful results. The idea of expressing the adequacy of resources in monetary terms should not be fetishized, as money alone will not solve the problem. Gartner put the issue bluntly: the amount spent on cybersecurity does not reflect the level of protection.[26] More important than the question of how much should be spent on cybersecurity is the question of where the resources should be allocated so as to have the most meaningful impact. Responses to the JIU questionnaires suggest inconsistent approaches to the prioritization of cybersecurity spending, which increases the risk of an inefficient use of already scarce resources. A highly persuasive, if somewhat complex and customization-intensive option for rightsizing cybersecurity investments is to follow a stringent methodology such as the Sherwood Applied Business Security Architecture (or an equivalent tool), which is based on the notion of bidirectional traceability. That is, the enterprise security architecture under this approach is set up in such a way that every business requirement is addressed by at least one corresponding security control, and every security control can be mapped back to a stated business requirement for security.[27] WIPO already uses this methodology, which has also been discussed in the context of the Information Security Special Interest Group and, **in the view of the Inspectors, is worth exploring further as a means of keeping cybersecurity investments firmly grounded in and linked with business requirements and sound risk management practices, thereby avoiding both overinvesting and underresourcing a key business continuity function.**

[26] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.

[27] Further information about the Sherwood Applied Business Security Architecture is available at https://sabsa.org/sabsa-executive-summary.

Box 7: Open-source solutions may provide cost-effective alternatives

Open-source software is a software development and distribution model that has become an integral part of the ICT industry. Some tools based on open-source software are widely used in the cybersecurity domain and include aspects such as threat intelligence sharing, identity and access management, network analysis and intrusion detection and prevention, incident response and forensics. Some examples of open-source software are even renowned as leading resources in their respective categories.

While responses to the JIU questionnaire suggest that some participating organizations are already complementing their commercially procured and in-house developed solutions with open-source software, there may be an opportunity for increased use of such options by United Nations entities. They may provide suitable solutions, particularly for organizations operating under circumstances marked by a scarcity of resources.

As with any proprietary product, open-source solutions should be evaluated on their own merits, but there are certain general advantages that are frequently associated with well-maintained open-source software products, such as transparency, security, the lower cost of licenses and fees, the use of open standards and the limited danger of vendor lock-in.

Although the use of open-source software does not normally involve licensing costs, this does not mean that it is totally cost-free. Its installation, configuration and maintenance, and the associated technical mastery required, imply staffing time and therefore costs. The full cost of ownership of such platforms may not be obvious for organizations with limited technical resources and experience with the deployment of such applications, although this limitation often applies – to varying degrees – to commercial products as well.

Organizations need not think only in terms of pure proprietary or pure open-source models. There are products based on a hybrid model aimed at combining the best of both worlds, namely the freedom and transparency of the open-source approach and the structured support provided by agile vendors. Another option is to use both proprietary tools and open-source software for different functions and purposes within an organization.

J. Investing in dedicated and specialized human resources

The information security function is not present in all participating organizations

110. **Responsibilities associated with cybersecurity go beyond technical expertise.** The majority of participating organizations have invested in hiring specialized expertise to cover the different dimensions of cybersecurity, sometimes placed under the leadership of a dedicated chief information security officer. The core aspects falling within the responsibility of the associated function include the elaboration of controls at the operational level on the one hand and management guidance at the strategic level on the other hand, with the aim of achieving the protection objectives of cybersecurity as reflected in the definition referred to in the present report. As such, the scope of the function extends beyond the digital sphere and is not limited to providing technical know-how. It involves diverse tasks, such as: developing and communicating a corporate regulatory framework (policy-setting and communication); providing advice on how to identify and manage risks (risk management); collaborating with business units in conducting risk assessments and business impact analyses (coordination and analytical role); investigating major breaches (investigative and analytical capability); and recommending as well as implementing appropriate control improvements (operational and technical expertise).[28] This description of tasks implies that the role includes a managerial

[28] See SFIA Foundation, *Skills Framework for the Information Age (SFIA) 7*, 2018.

dimension, both within and outside of the ICT environment, and requires operation in close cooperation with a wide range of stakeholders, particularly the business units of the organizations. The authority delegated to the chief information security officer (and cybersecurity experts more generally) to communicate and compel action across the organization therefore becomes paramount.

111. **Internal capacity varies.** According to JIU research, at least 16 participating organizations have built specialized and dedicated human resource capacity in-house, ranging from a single information security officer, sometimes assigned only part-time, to a larger organizational unit headed by a chief information security officer, generally at the P4 or P5 level (annex V). In contrast, in 10 participating organizations, cybersecurity tasks are handled mainly by ICT officers among their other duties. There is a high incidence of using external expertise due to the complex technical nature of the domain, which is evolving constantly and requires a considerable degree of specialization that is challenging and costly to keep available and current on a permanent basis. As a result, such expertise is often supplemented by hiring temporary resources, including consultants and contractors, or by subscribing to the services of commercial providers or those of the United Nations International Computing Centre. Some interlocutors pointed out that the global dearth in experienced cybersecurity practitioners featured among the biggest challenges faced by the United Nations system organizations in setting up, maintaining and managing their cybersecurity programmes. To provide an alternative for entities that are not in a position to immediately establish a dedicated function, the Inspectors wish to highlight that the United Nations International Computing Centre offers a service titled "security governance", sometimes also referred to as "chief information security officer as a service", which is presently subscribed to by six participating organizations, with another four having availed themselves of this service in the past. **The Inspectors are of the view that United Nation system organizations need to address future cybersecurity expertise requirements through proper human resource planning, particularly since the knowledge, skills and abilities to address cybersecurity risks and challenges are specific and may not be easy to attract and retain.**

112. **Investing in dedicated capacity is worth considering.** Noting that corporate arrangements should ideally be reflective of the size of the organization and its specific requirements based on the risk assessment conducted and the cyberenvironment in which the entity operates, the reality is that other factors may be more decisive. Specifically, disparities in the internal set-up observed by the Inspectors across the participating organizations may be more indicative of the constraints each one is facing rather than a deliberate or strategic choice. As a matter of fact, in four participating organizations the cybersecurity function was considered nascent at most, which may indirectly put the entire system at risk. **The Inspectors believe that having dedicated and specialized cybersecurity expertise within each organization contributes to reinforcing the posture not only of that organization but of the system as a whole and is therefore a worthwhile investment.** As with other functions associated with the core business of organizations, building durable internal human resources capacity for the protection of information and cyberassets, where possible, is generally to be favoured over reliance on successive temporary resources, not least because of additional risks associated with their use and the limited enforcement capacity that organizations have over affiliated personnel (para. 100). Furthermore, **instituting a regular chief information security officer position to oversee and manage such expertise may bring the necessary focus and coherence in approach and would, in the Inspectors' view, contribute to strengthening the cyberresilience of the organizations concerned.**

113. **No generally accepted organizational placement for cybersecurity.** The most appropriate placement of cybersecurity in terms of reporting lines is a question that has been debated within the United Nations system and beyond, and one for which there is no definitive, universally applicable response. International standards do not provide authoritative guidance and leave it to each organization to decide the most appropriate placement in accordance with its needs and architecture. In the United Nations system organizations, in the majority of cases,

the function is placed within the ICT department, generally reflected by a direct reporting line to the head of the department or equivalent. This predominant structural arrangement may be seen as a legacy from the past but reflects the reality that cybersecurity tends to gravitate naturally towards ICT, based on the technological awareness and expertise required to manage related information systems and other protective infrastructure. In addition, the ICT department is often the one devising and implementing the operational response in the event of a cyberattack, and decoupling the two may lead to efficiency losses.

114. **Managing divergent organizational priorities between the ICT and cybersecurity functions.** Notwithstanding the above, placing the officer or team in charge of cybersecurity under the authority of the head of the ICT department may create tension between the respective main objectives pursued by each role, with risk management and information security being the key concern for the chief information security officer versus operational and cost effectiveness as well as speed of delivery for the head of ICT. The potential conflict of interest is evident, yet far from straightforward to resolve. An overly operationally minded approach to cybersecurity (such as that associated with ICT professionals) may multiply the negative impact on delivery further down the line when cyberrisks that were potentially brushed aside earlier start materializing. At the same time, an all too risk-averse attitude (such as the one ascribed to cybersecurity professionals) may unduly paralyse operational agility and impede mandate delivery in other ways. Managing and resolving tensions between different organizational objectives, and specifically their resource implications, is part of the day-to-day tasks of every manager, and executive leadership is best placed to strike a balance in this regard.

115. **Empowering the cybersecurity function.** Irrespective of the organizational placement of cybersecurity, **the Inspectors stress that it is important to safeguard the opportunity for cybersecurity considerations to be voiced and heard by the responsible decision makers without restriction.** The function should be situated where it can address executive management independently and effectively contribute to other corporate frameworks such as enterprise risk management, information and knowledge management, physical safety and security, and oversight, as argued throughout the present report. This is most effectively achieved when a strong internal multi-stakeholder governance mechanism involving all relevant departments is in place. Some well-elaborated examples of such multi-stakeholder and multi-tier governance mechanisms were provided by WIPO and ICAO.

116. **Specialized training.** Irrespective of who is put in charge of cybersecurity within an organization and whether the function is concentrated in one person or a team or scattered across several part-time resources, it is important that specialized training remains available to all ICT staff with security-related responsibilities, so as to ensure continually updated know-how and skills. Such training for ICT staff, such as developers or systems administrators, is reportedly already available in most of the organizations and should be further encouraged (figure VII). A solid cybersecurity training programme and, where appropriate, a certification process for select ICT officers should ideally be a core component of the workplan of their department, complemented with a secured budget. Without some resources set aside for the purpose of continuous skills upgrades, ICT staff are left to maintain their professional knowledge at their own initiative or through their participation in professional communities. This approach relies too heavily on individual professional attitudes and is unlikely to be sustainable. The Inspectors welcome the statements by several organizations about their intention to reinforce this area but note that, even in cases where the level of resources allows for such specialized training to be offered, most of the time it is done on an ad hoc basis and without long-term training objectives or a systematic approach. Particularly in cases where there is no dedicated human resource capacity allocated to manage cybersecurity in a consistent manner, adequate training opportunities for staff who are asked to cover relevant components become all the more important.

A security operations centre brings coherence in cybersecurity operational response

117. **Main functions of a security operations centre.** A security operations centre is an organizational unit that is focused on day-to-day cybersecurity operations. While there are inevitable differences between its various incarnations, the broadest possible mandate puts the centre in charge of monitoring the security of an entity by preventing, detecting, analysing and responding to cybersecurity incidents. Cybersecurity experts often say that a security operations centre is made of people, technology and processes and is the central hub for collecting, correlating and analysing information streams from various real-time sources. The internal information collected and processed by a such a centre can include data from sources such as network devices, servers and hosted applications, desktop computers and mobile devices, physical security systems, and specialized security appliances. A security operations centre also collects and processes threat intelligence from external sources, usually consulting a combination of open-source (including publicly available government information) and commercial threat intelligence, which is correlated with internally collected data and analysed for signs of emerging threats. Given the complexity of tasks and diverse expertise required, setting up and maintaining a fully equipped and functional security operations centre can be a complex and costly undertaking. Whether such a centre is necessary to have and, if so, whether it should be set up in-house or procured from an external provider are questions to be answered for each organization in the light of its own requirements.

118. **In-house, outsourced or hybrid solutions for security operations centres: diverse set-ups observed across organizations.** There are divergent views among participating organizations about the advantages and disadvantages of in-house versus external solutions, which is evidenced by the diversity of arrangements and practices the Inspectors found during their review. Some organizations rely on a virtual or distributed security operations centre in the sense that some of its functions are spread across a decentralized pool of staffing resources. A number of entities have made the decision to build their own in-house centre, while others are using an external one sourced from commercial providers or sharing a centre with other entities through the United Nations International Computing Centre's related service, either exclusively or in combination with a core in-house capacity. The organizations that use such hybrid solutions have, in some cases, drawn a line between strategic and oversight-related functions, which remain internally managed, while operational control, particularly when an around-the-clock ("24/7") monitoring capacity is involved, is relinquished to external providers. A few even use more than one security operations centre, which allows them to segregate certain portions of particularly sensitive data from the data sets entrusted to be managed by external outfits. The Inspectors noted that a few participating organizations were currently considering the creation of a security operations centre as an option.

119. **Elements considered for security operations centre arrangements.** Arguments in favour of an internal centre include the ability to react more quickly to threats and vulnerabilities and to exercise better control of end point devices, admittedly at a higher cost. The latter is said to be achieved through more direct visibility of such devices and their status, with the possibility to remediate risky end point posture in real time. Moreover, an internal centre is considered to be an effective way to centralize cybersecurity functions, which, according to a broad industry consensus, leads to improved cyberresilience overall. For many United Nations system organizations, the cost of running an in-house security operations centre can reportedly be prohibitive, and the benefits gained may not be commensurate with such organizations' cybersecurity profile and associated protection requirements. Only a small number of United Nations entities can afford to maintain a full-fledged cybersecurity programme to deal with and respond to threats autonomously, relying only on internal capacity. Moreover, even if they manage to put adequate structures in place, they may still fail to sustain a standing, on-call force of multi-skilled and trained cybersecurity experts who can respond to complex cyberattacks, which tend to be infrequent and irregular, implying some fluctuation in the expertise required. In addition, some organizations consider that maintaining a full internal

capacity to manage all operational tasks cannot match the expertise of external specialized providers, who also tend to be better resourced to invest in development and research considered indispensable for the dynamic field of cybersecurity. At the same time, even where entities opt for outsourcing, the point has been made that there needs to be a sufficient level of in-house capacity and representation of some of the core cybersecurity functions inside the entity, which has expert knowledge of internal workflows and processes and can also serve as an effective interface with the external provider. In cases where external security operations centres are used, vendor management also becomes a key preoccupation and must be ensured thorough vetting, adequate legal protection clauses in contracts, and the avoidance of vendor dependency or "lock-in". Some of the considerations for or against outsourcing of a security operations centre may also apply in relation to other decisions regarding the use of internal versus external capacities to manage cybersecurity and are summarized in box 8.

Box 8: Using external providers for a security operations centre and other cybersecurity services

Pros:

- Ensures the availability of diverse, current and highly specialized skill sets and tools
- May lead to cost efficiency
- Offers the possibility of scaling up or down according to the ever-changing threat landscape and fluctuating capacity requirements
- Perceived neutrality and impartiality

Cons:

- Exposure to vendor dependency ("lock-in")
- May encounter difficulty customizing standardized services and solutions, leading to suboptimal and rigid solutions
- Increased reliance on unknown or unvetted staff placed under the direct control of managers
- Potential exposure of sensitive data to third parties
- Limited transparency about reporting incidents
- Costs

120. **A security operations centre improves coherence of cybersecurity response.** Each organization should assess whether to pursue the establishment of a such centre based on a cost-benefit analysis involving parameters such as the complexity of its ICT infrastructure set-up, the number and type of critical assets and processes managed, and the overall volume of data flows, and hence the threat frequency, which may suggest different levels of need for constant monitoring and protection. The Inspectors wish to highlight that one of the important aspects of a formal security operations centre – regardless of its size and capacity – is the focus and coherence it provides for day-to-day monitoring and operations in an organization. Even if it is a very small team that needs to draw on ICT staff located elsewhere in the organization, or on external providers, it can still perform a crucial coordination and synchronization role and raise organizational awareness. **The Inspectors therefore suggest that executive heads consider the option of creating a security operations centre or streamlining existing capacities into an equivalent mechanism based on a critical review of their corporate needs and of the in-house and external capacities already at their disposal, and that they ensure that they are**

able to fully substantiate the reasons underpinning their decision for or against instituting a security operations centre.

K. Reflecting and reporting on organization-wide efforts towards improved cyberresilience

121. The degree to which the elements detailed in the present chapter are reflected in an organization's approach to cybersecurity directly influences its posture and capacity to identify, prevent and detect cyberthreats, as well as to respond to and recover from incidents. Mindful of the fact that the arrangements in place may be driven by strategic or operational choice or dictated by other considerations, executive heads should initiate an organization-wide review to study the extent to which each of these elements is integrated in the policies and practices of their organization.

122. The implementation of the following recommendations is expected to enhance the effectiveness of the preparedness and response of the United Nations system organizations in the area of cybersecurity.

Recommendation 1

The executive heads of the United Nations system organizations should prepare, as a matter of priority and no later than 2022, a comprehensive report on their cybersecurity framework and present it to their respective legislative and governing bodies at the earliest opportunity, covering the elements contributing to improved cyberresilience examined in the present report.

123. The conclusions of such an internal review should be reported to the legislative and governing bodies, considering the strengths and weaknesses identified and suggesting measures to further reinforce cyberresilience. In the Inspectors' opinion, legislative and governing bodies would then be in a better position to provide high-level strategic guidance with reference to an explicit statement on the risk appetite regarding cybersecurity matters and to allocate resources towards attaining the desired level of protection. As stated above, executive management should consider reporting regularly on cybersecurity matters to the legislative and governing bodies. The Inspectors acknowledge that some portions of the information presented in such a report may be sensitive and may need to be treated with the appropriate level of confidentiality. **Executive management is therefore advised to take the utmost care in selecting a format and channel of reporting that provides sufficient insight to the respective legislative and governing body without jeopardizing the defences of the organization.**

Recommendation 2

The legislative and governing bodies of the United Nations system organizations should consider the reports on the elements contributing to improved cyberresilience prepared by the executive heads and provide strategic guidance on further improvements to be implemented in their respective organizations, as necessary.

IV. Cybersecurity from a system-wide perspective

A. Cybersecurity – a system-wide priority?

124. **System-wide collaboration on cybersecurity – a long-stated priority.** Strengthening the cybersecurity posture of the United Nations system has been stated as a priority, both by Member States and by United Nations officials at the highest possible levels, for many years. For example, in 2008, the General Assembly encouraged the Secretary-General, as the chairperson of CEB, to foster deeper coordination and collaboration among United Nations organizations in all matters related to ICT, enterprise resource planning, and – notably – security, disaster recovery and business continuity.[29] In 2013, the Advisory Committee on Administrative and Budgetary Questions, in reviewing a report on the progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat, encouraged the Secretary-General to continue to pursue system-wide collaboration and seek all options for further cooperation and sharing of solutions for information security among the organizations of the United Nations system.[30] More recently, in 2019, as part of the conclusion of a discussion at the CEB level, the Secretary-General himself emphasized the importance of strengthening the United Nations system's own capacity to protect itself from cyberattacks.[31] The underlying assumption in this regard has been that greater collaboration at the system-wide level, including joint approaches and shared operational solutions, is among the key factors to achieving a better level of protection for the system as a whole.

125. **Attempts at a joint strategic approach.** As stated, United Nations system organizations mostly face the same challenges and threats in the cyberenvironment, which would imply that there is a potential for devising a joint approach in response. Considering that the security of the system depends, at least partly, on the security of its members individually given their interconnectedness at various levels, there is also a solid reason for doing so. During the preparation of the present review, several participating organizations pleaded for the elaboration of a common strategy owned, implemented and reported on by agencies as partners acting in concert and driven by the common objective of achieving a certain maturity level across the system, on the basis of a set of minimum criteria to be met by all. A request to develop a system-wide cybersecurity strategy in order to help create a basis for consistent cybersecurity practices throughout the system appears in the 2017 records of the Information and Communication Technologies Network.[32] However, the initiative does not seem to have materialized or to have been pursued further in any tangible sense. Another attempt towards promoting a harmonized approach included a proposal to survey organizations on a yearly basis on their cybersecurity measures, so as to produce an internal benchmark of maturity and better assess the system's overall exposure to risk. Despite significant preparatory work that included two pilot survey rounds conducted among some 20 organizations over the course of 2018 and 2019, the proposal failed to attract the collective support of senior management levels at the time. The main arguments put forth when rejecting such benchmarking efforts were, on the one hand, the diversity of organizational set-ups and contexts limiting the value of a collective assessment and, on the other hand, the limited preparedness of entities to share their internal cybersecurity assessments outside of their organization, effectively citing cybersecurity risks as the main obstacle for pursuing even a cumulative assessment. Opinions expressed during interviews suggested that the COVID-19 pandemic might have brought about a change in perceptions and mindsets regarding cybersecurity and that proposals formerly considered ambitious or unrealistic might stand a greater chance of generating interest and being welcomed

[29] General Assembly resolution 63/262.
[30] A/68/7/Add.11, para. 6.
[31] CEB/2019/2, para. 39.
[32] CEB/2017/HLCM/ICT/9, pp. 7–8.

today. In fact, a debate about the opportunity to apply a reference maturity model similar to the one recently adopted by the CEB Risk Management Forum appears to have resurfaced in the context of the latest inter-agency meeting among cybersecurity experts.

126. **Collective responsibility to ensure a minimum level of defence.** Aiming for full system-wide harmonization, particularly based on conclusions drawn from a comparative maturity assessment across organizations, may indeed be overambitious and even beside the point. As stated by the think tank Gartner, trying to compare corporate cybersecurity arrangements and measures against each other may enable statements to be made regarding the relative maturity of each organization but does not give any reliable indication about the absolute level of protection of any of them.[33] Reputational as well as operational cross-dependencies between the United Nations system organizations, however, make it their collective responsibility to raise the bar as high as possible for everyone and help each other to reach it. It should be noted that it was particularly those organizations with an advanced cybersecurity framework and strong internal or external capacity who were most supportive of related efforts. It is a thin line to walk, but it is crucial that the system find the right balance between participating organizations' respective requirements, their existing arrangements, and a system-wide approach to determining a minimum standard to be attained by and for the benefit of all. **In the view of the Inspectors, determining a basic level of protection and minimum defence requirements for the United Nations organizations, and therefore for the system as a whole, remains a valid objective that continues to be worth pursuing**.

127. **Efforts to institute a shared capacity at the operational level.** The issue of a federated system-wide capacity for preventing, detecting and responding to cyberthreats and attacks has been debated a number of times at various levels. Almost 10 years ago, the Information and Communication Technologies Network issued a road map for establishing a United Nations computer incident response team.[34] This initiative did not materialize, as no agreement could be reached on the funding model at the time. More recently, the Information Security Special Interest Group resumed its work on assessing the feasibility of a shared security operations centre among United Nations entities, yet the discussion among its members highlighted a host of remaining challenges (cost apportionment, alignment with varied pre-existing capacity, agreement on the expected scope and prioritization of support in the event of a widespread attack, etc.). These efforts were predicated on the expectation that a system-wide incident response capacity would have the potential to realize significant efficiency gains while also offering increased protection, especially for organizations that could not afford to maintain a standby capacity for the eventuality of an attack that might nevertheless hit at any time. However, these attempts illustrate that the objectives, while clear and well supported, are more difficult to translate into practice than one might anticipate. Experience shows that the moment they reach a certain level of concretization, their implementation becomes elusive.

128. **Training and awareness-raising as an ambivalent candidate for system-wide resource pooling.** One example of a promising proposal that proved somewhat ambivalent on closer inspection was the area of cybersecurity training and awareness-raising. The question of collaboration on learning programmes in the United Nations system was reviewed in a recent JIU report.[35] One of the findings was that there was significant duplication of efforts in the creation of similar programmes by different organizations. At first glance, training and awareness-raising resources on cybersecurity seem like a natural choice for system-wide collaboration and resource pooling. Based on the assumption that most end user training can be standardized, since a large portion of the related learning material does not have to be organization-specific due to the shared threat landscape, one of the first joint projects completed by the Information Security Special Interest Group involved the development of core components of a common cybersecurity curriculum for adaptation and use by its members. The

[33] Gartner, *The Urgency to Treat Cybersecurity as a Business Decision*, February 2020.
[34] CEB/2013/5, paras. 38–39.
[35] JIU/REP/2020/2.

curriculum approach appeared to have gained some traction with a number of organizations, which chose to adopt the online information security awareness training module of the United Nations Secretariat or used the United Nations International Computing Centre and its information security awareness service to customize and tailor related content. However, the Inspectors did not detect a strong consensus among participating organizations regarding the benefit of a common approach to training. In fact, several organizations argued strongly against a standardized approach, specifically citing mandate-related specificities or the constraints imposed by the often lengthy collective development process that quickly rendered jointly developed content obsolete and was not easily substituted, while also necessarily converging around a "lowest common denominator" approach that might not live up to the expectations and requirements of the users without considerable subsequent investments needed for further tailoring and expansion. In the light of these considerations, a number of organizations have developed their own training modules, sometimes in cooperation with external providers, at a cost that is not insignificant. **The Inspectors remain convinced that United Nations system organizations would benefit from some harmonized training, even if it might need to be tailored for some organizations.**

129. **Optimizing resources for cybersecurity.** There was consensus among all experts and managers interviewed about the fact that the United Nations entities individually and collectively were small actors compared to entities from the private sector, and that resources available to them to face and respond to more sophisticated external attacks by organized crime or other sponsored attacks were at best limited. At the same time, participating organizations often allocate resources to cybersecurity in isolation and for their own purpose, sometimes under pressure in response to a specific event. There is a strong sense within the system that there are efficiencies to be gained by approaching cybersecurity in a joint fashion. However, the responses from JIU participating organizations on areas where the pooling of resources could be feasible and useful generated divergent feedback. One area that received support as a source for potential cost savings was closer coordination around the engagement of external service providers, specifically commercial and private sector entities. Many organizations confirmed using such providers, often naming the same companies for the same or similar services, including for risk or vulnerability assessments, ISO 27001 audits, or for specific software solutions, implying that each of them had subjected these companies to their respective internal screening and vendor management procedures while also paying them separately. Only a handful of organizations indicated that they benefited from memoranda of understanding or similar arrangements between them to draw on each other's procurement processes or contracts for services related to cybersecurity protection and response, despite the existence of a mutual recognition agreement signed by 20 organizations. The Inspectors recognize that there are factors limiting a large-scale implementation of such joint initiatives but that these initiatives nevertheless warrant increased attention to realize efficiency gains. A number of challenges to joint procurement and to collaborative procurement in general were identified by the Inspectors through interviews and the questionnaire. The different procurement procedures and rules in the system form barriers and limit the application of collaborative procurement. However, some obstacles are not related directly to rules and procedures but rather to the operating culture of the organizations, which may not allow open cooperation, instead favouring strict organizational control. In this context, some barriers include the differences in operating philosophy between highly centralized and decentralized procurement, differences in funding modalities (such as advance payments) and a lack of alignment in ICT systems and in accounts payable systems, as reflected in a JIU report on procurement-related matters.[36] At the very least, if the joint procurement of certain services proves not to be feasible, participating organizations should do everything in their power to coordinate their efforts as much as possible. Otherwise, through inconsistent procurement practices, they run the risk of incentivizing commercial providers to charge different fees for the same service across the system, creating a form of

[36] See JIU/REP/2013/1.

competition that only benefits those providers while being detrimental to the financial interests of the organizations concerned.

130. **No truly concerted effort at system-wide level beyond coordination and partial operational solutions.** The significant prominence and momentum that cybersecurity has gained at the highest levels could be said to have created optimal conditions for a forceful push in the direction of establishing system-wide capacity. However, despite the existence of several important resources, mechanisms and initiatives available within the system, including apparent political will, evidence of progress in making these aspirational statements a reality has been far from obvious. At this point in time, there is no single entity formally tasked with driving the agenda of a harmonized approach to cybersecurity, nor for developing and implementing shared solutions for United Nations system organizations. Presently, system-wide efforts on cybersecurity are concentrated institutionally around inter-agency coordination mechanisms under CEB, and they are operationally supported, to a degree, by the United Nations International Computing Centre as a provider of certain shared services for several United Nations system organizations. In the present chapter, the Inspectors examine the respective institutional and operational arrangements, including what appears to be a degree of disconnect between them, and the prevailing inter-agency dynamics on this matter (annex VI). The Inspectors further seek to identify the progress achieved so far, the benefits and limitations inherent in the current set-up, and areas where there may be potential for stronger collective action in devising responses by the United Nations system as a whole, to the extent practical and reasonable.

B. Inter-agency mechanisms dealing with cybersecurity

131. **Long history of attention from inter-agency mechanisms.** Cybersecurity has, under the heading "information (system) security", featured in the information technology discourse at the system-wide level since the time of the Administrative Committee on Coordination. As early as 1994, a task force established by the predecessor of the Information and Communications Technology Network (known since 2018 as the Digital and Technology Network) was entrusted with reviewing a set of "information system security guidelines for United Nations organizations" published in 1992,[37] suggesting that there had been considerable attention and effort invested in the matter even earlier. It should be noted that the guidelines represent a comprehensive and surprisingly progressive effort to map and provide guidance on the diverse dimensions of cybersecurity, both at the managerial and operational levels, and the somewhat dated terminology used in the document should not distract from the fact that a non-negligible portion of its contents and recommendations remain of relevance even 30 years on.

132. **Sustained interest in a coordinated approach to cybersecurity.** The idea of a coordinated response to cyberthreats still featured in official records 10 years later, in 2002, when the members of CEB recognized that, "although organizations' security needs fall into different categories (some having extremely confidential and sensitive data banks), there were important issues common to all organizations which had to be addressed with all urgency."[38] In 2010, the term "information security" appears to have been superseded by "cybersecurity", which gained significant momentum when the case was again made for defining a "blueprint for a system-wide approach" to cybersecurity, describing the implications of cyberthreats on "all sectors" as a "possible cybertsunami".[39] In subsequent years, similar statements were made at the level of the High-level Committee on Management with regard to detecting "considerable common ground with respect to how to best protect [the United Nations system organizations]

[37] Advisory Committee for the Co-ordination of Information Systems, "Information System Security Guidelines for the United Nations Organizations", New York, 1992.

[38] CEB/2002/HLCM/10, para. 8.

[39] CEB/2010/1, para. 53.

from business disruptions and security threats",[40] while the Information and Communication Technologies Network stated that "enhancing the capacity of agencies to resist cyberthreats must remain a priority."[41]

133. **Landmark system-wide documents on cybersecurity and cybercrime adopted in 2013 and 2014.** In 2010, CEB tasked the High-level Committee on Management and the High-level Committee on Programmes with taking up the issue jointly under the leadership of ITU and the United Nations Office on Drugs and Crime (UNODC), later joined by the United Nations Conference on Trade and Development (UNCTAD), UNDP and UNESCO. This cross-cutting initiative culminated in the endorsement of the United Nations-wide framework on cybersecurity and cybercrime in 2013[42] and, building on that framework, the United Nations system internal coordination plan on cybersecurity and cybercrime in 2014.[43] Even though both documents focus predominantly on the "outward-facing" dimension of the work of the United Nations (that is, programmatic activities designed to support Member States in their endeavours on the subject), they provide a solid starting point for framing the "inward-facing" dimension of cybersecurity for the system (box 9). Nevertheless, the Inspectors noted that not a single participating organization made reference to the framework or the plan during the preparation of the review. While the plan as such did not appear to have become a lasting point of reference for the system, the Inspectors were reassured that the core principles and elements contained therein continued to inform the workplan of the relevant inter-agency bodies active in the sphere.

Box 9: System-wide framework and internal coordination plan on cybersecurity and cybercrime

Endorsed by CEB at its second regular session of 2013, the United Nations-wide framework on cybersecurity and cybercrime lays the groundwork for coordination among United Nations system organizations in response to concerns of Member States regarding cybercrime and cybersecurity.

The framework:

- Introduces some common definitions of key concepts and sketches out the scope of the subject matter
- Highlights the intersection between the related mandates of the entities concerned
- Establishes basic principles for programme development and technical assistance related to cybercrime and cybersecurity
- Contains guidance on enhanced cooperation in the delivery of technical assistance to Member States in this regard.

Building on the framework, the United Nations system internal coordination plan on cybersecurity and cybercrime was designed in 2014 to guide internal coordination among United Nations system organizations in the area of cybersecurity and cybercrime, centred around five topics highlighted by the Secretary-General for possible joint action across the system. For each topic, the plan outlined an array of common principles and action points that organizations were invited to adopt. In particular, executive heads were encouraged to develop and launch a mandatory computer-based training course on cybersecurity for staff, based on a training syllabus agreed by the Information and Communication Technologies Network, and to establish a cross-organizational computer incident response team. These

[40] CEB/2013/5, para. 36.
[41] CEB/2013/2, para. 58.
[42] Ibid., para. 85 and annex III (United Nations-wide framework on cybersecurity and cybercrime).
[43] United Nations system internal coordination plan on cybersecurity and cybercrime, November 2014, internal document.

were also the action points considered to be of relevance to the High-level Committee on Management's work by its Chair (CEB/2014/5, para. 72).

The following topic is of particular relevance to the present review:

Topic 1: Ensure effective internal preparation to cope with cyberthreats, among individual agencies and across the United Nations system, including policy and resource obstacles that may prevent agencies from acting together to jointly protect the United Nations system better through, for example, the inclusion of cybersecurity in risk assessment and risk management frameworks.

134. **The Information Security Special Interest Group as the main system-wide expert forum on cybersecurity.** Overall, the inter-agency machinery dealing with cybersecurity in the United Nations system was found to be long established and generally functioning. The Information Security Special Interest Group, created in 2011 as the principal mechanism within the United Nations system for the promotion of inter-agency cooperation and collaboration to optimize information security within its member organizations, reports to and receives direction from the Digital and Technology Network and operates under the overall guidance of the High-level Committee on Management. Based on its terms of reference, its membership is explicitly restricted to the chief information security officers of CEB member organizations or the equivalent. In cases where no such function exists, it is usually an ICT officer who represents the respective organization. The Information Security Special Interest Group's working methods include an annual symposium with the participation of external speakers, an executive session for formal decision-making held during the annual symposium, and time-bound working groups with lead organizations volunteering to drive deliberations on topics of interest. Several non-CEB member organizations participate in the work of the Information Security Special Interest Group as observers without voting rights, among them the United Nations International Computing Centre. The group is chaired on a rotational basis by one of its formal members, which at the time of writing the present report was a role assumed by the Office of Information and Communications Technology of the United Nations Secretariat.

135. **Utility of main inter-agency body as forum for exchange confirmed.** The Information Security Special Interest Group has acquired considerable professional credibility as the official forum where United Nations cybersecurity practitioners come together on a regular basis to discuss challenges, opportunities and good practices for the system as a whole. A content analysis of recent reports of the Information Security Special Interest Group symposiums confirms that there is rich debate and attention within the Group to a wide range of operational and strategic issues, such as cloud security and cloud risk management, digital identity management, the benchmarking of cybersecurity maturity, information security awareness training and, more recently, the idea of a shared security operations centre as well as the consolidation of threat intelligence services. In fact, in their response to the JIU questionnaire, some two thirds of the participating organizations said that they saw the Group as effective in promoting cooperation and collaboration among United Nations entities and valued the substantive contributions of its members as well as the opportunities for exchange with external, including private sector, experts. The efforts of the Chair in facilitating professional debate and driving progress on the Group's work plan were commended by many members. Some weaker aspects related to the Group's functioning are already being addressed, such as the low frequency of the Information Security Special Interest Group symposiums and limited interactions in between sessions, which, according to some members, should be increased to facilitate more continuous and informal dialogue. Responding to a clear need in this regard, a dedicated instant messaging channel for direct informal exchange between members of the Information Security Special Interest Group was set up for prompt communication and the sharing of information as and when necessary. Efforts supporting day-to-day exchanges have

been mentioned favourably by chief information security officers, who also confirmed having used such channels actively in their daily work.

136. **Inter-agency machinery seized with cybersecurity at all levels.** From the Information Security Special Interest Group itself to the Digital and Technology Network and the High-level Committee on Management, there was evidence that cybersecurity was being actively debated and recognized as critical. At the level of the Digital and Technology Network, which brings together the heads of ICT departments and receives the reports and recommendations of the Information Security Special Interest Group for endorsement and forwarding to the High-level Committee on Management, "information security and cybersecurity" is listed among the 10 objectives of the Network contained in its revised terms of reference of 2019.[44] In practice, the Digital and Technology Network can be said to have been generally appreciative of the work of the Information Security Special Interest Group, as only in a handful of cases has the Digital and Technology Network deviated from the position taken by the Information Security Special Interest Group, and most of the Group's recommendations have been endorsed, sometimes with modifications. At the level of the High-level Committee on Management, which played an important role in the development of the 2013 framework and the 2014 coordination plan, cybersecurity has featured in the Committee's strategic plans, including its most recent one (2017–2020), as an element of the strategic priority of risk management and resilience-building. The latter features a statement indicating that the High-level Committee on Management will engage in a renewed effort to promote cyberthreat monitoring and response, including the implementation of mitigation measures, on a system-wide level.[45] However, the records of the High-level Committee on Management, though clearly cognizant of cybersecurity as an issue of concern in general terms, show that specific recommendations and items related to the topic rarely reach the Committee. In this context, the Inspectors note that, in their response to the JIU questionnaire, only one third of the participating organizations said they saw the Information Security Special Interest Group as effective in generating momentum for action at the upper levels of the CEB machinery.

137. **Implementation of the advice and guidance of the Information Security Special Interest Group is reliant on its members.** During the present review, the Inspectors found that inter-agency coordination and collaboration on cybersecurity in the United Nations system had yet to produce the expected results. While a considerable amount of conceptual work is being advanced on a yearly basis through the Information Security Special Interest Group, and the issue has the attention of senior management, progress towards shared solutions, common or concerted approaches and joint projects has been slow to materialize. For context, it is worth recalling that the latest iteration of the terms of reference of the Group, as revised in 2018,[46] reflects its commitment to sharing knowledge, experiences and solutions and notably includes the implementation of joint projects. In fact, later that year, on the occasion of the Information and Communication Technologies Network transitioning to become the Digital and Technology Network and revisiting the mandates of each of its subgroups, the newly renamed Network went even further in deciding that, in addition to advancing inter-agency collaboration and knowledge-sharing in the area of information security, it was necessary for the Information Security Special Interest Group to become more active in the design and delivery of shared solutions and innovation.[47] However, the vision of the Digital and Technology Network for its subgroup to engage in more hands-on solution development for the system does not appear to be matched by any level of operational capacity independently of its members' internal resources and individual level of engagement in this regard. The Information Security Special Interest Group is de facto lacking an effective mechanism to facilitate implementation and joint delivery of the solutions devised or the agreements reached in the inter-agency context. Noting that it is not primarily the responsibility of a coordination body to be concerned with

[44] CEB/2019/HLCM/DTN/03/R1, p. 2.
[45] CEB/2016/HLCM/15, p. 13.
[46] CEB/2018/HLCM/ICT/3/Rev. 1.
[47] CEB/2018/HLCM/ICTN/18, p. 6.

implementing its own recommendations, the absence of an officially sanctioned "operational arm" for the system as a whole that takes direction from the collective of chief information security officers and serves the common interest is, in the Inspectors' view, among the key factors hindering progress towards a system-wide approach to cybersecurity. Whether other existing mechanisms or bodies can reasonably fill the implementation gap is examined in more detail in the ensuing sections of the present report.

138. **Empowerment of chief information security officers individually and as a group.** The profile of the Information Security Special Interest Group members was found to be uneven, ranging from working level to strategic level participation, with some chief information security officers holding entry-level positions in the professional category while others performed mid- to senior-level managerial roles or headed entire departments. Beyond the technical expertise and a frank culture of discussion that characterizes debate within the Information Security Special Interest Group according to its members, the heterogeneity of its membership reportedly affects the dynamics within the Group and has had a direct impact on the Group's capacity to provide authoritative guidance for the system. With each member being differently empowered within the structure of his or her respective organization and associated limitations to commit the entity in inter-agency contexts, opportunities to have a transformational role, both within that organization and collectively through concerted action across the system, are limited. The Information Security Special Interest Group as a coordination body faces the same challenges in this regard as any other inter-agency mechanism in the absence of decision-making authority to compel action directly at the system level, which is why it would be unrealistic to expect implementation to materialize within that forum. Concurrently, it has little influence over how the outcomes of its work are relayed to senior management within each organization. It is clear from the records of the Digital and Technology Network that these limitations are well-understood, as evidenced by the Network's call on its own members – the heads of ICT departments – to empower chief information security officers, among others, by delegating additional authority to them.[48] It is also worth recalling that the Information Security Special Interest Group itself reports to the Digital and Technology Network, thereby mirroring the prevailing set-up and associated challenges observed within most organizations where the chief information security officer reports to the head of his or her respective ICT department. To counteract the limiting effects of the current set-up, **the Inspectors reiterate their call for greater internal empowerment of the chief information security officer function where it exists, including its managerial scope and independence from ICT to the extent possible, and the creation of such a function where it does not exist.** With regard to the empowerment of chief information security officers as a group, the Inspectors observed that there was generally little appetite for elevating the Information Security Special Interest Group within the inter-agency machinery by decoupling it from the Digital and Technology Network and according it network status, which would enable the Group to report directly to the High-level Committee on Management. On the one hand, arguments against such a shift included the general proliferation of networks, task forces and coordination forums within the CEB machinery, which was, in itself, considered unlikely to contribute to the advancement or effective prioritization of the issue. On the other hand, the prevailing view seemed to be that the Information Security Special Interest Group already had an adequate and robust channel at its disposal to bring cybersecurity considerations to the forefront of strategic system-wide discussions through the Digital and Technology Network and the High-level Committee on Management. **The Inspectors reaffirmed that the Information Security Special Interest Group had effectively improved the sharing of information on cybersecurity in the United Nations system and should continue to play its role without changing the current architectural configuration. The Inspectors nevertheless point out the need to devise a mechanism that ensures that the Information Security Special Interest Group – as a separate entity – can provide strategic direction on behalf of CEB and the United Nations system.**

[48] See, for example, CEB/2017/HLCM/ICT/9, p. 8.

C. United Nations International Computing Centre as a cybersecurity service provider

139. **Revisiting the unrealized potential of the United Nations International Computing Centre.** In the context of its report on cloud computing in 2019, JIU has already called for further examining the conditions to better leverage the unrealized potential of the United Nations International Computing Centre and its diverse ICT service portfolio for the United Nations system. At the time, cybersecurity was highlighted as one of the areas where such potential was considered to be ripe for further study. However, with the broader perspective of the reform of United Nations business operations in mind, the Inspectors see room for a separate, more holistic review of the United Nations International Computing Centre and its overall functioning, business model, governance structure and mandate, possibly even beyond the confines of its established role as a provider of ICT services to its clients, which currently include but are not limited to United Nations system organizations. Since its creation in 1971, which was preceded by a detailed external audit report that was commissioned by the Secretary-General in his capacity as Chair of the relevant inter-agency coordination mechanism with a mandate to study the electronic data-processing facilities and needs of the United Nations and the specialized agencies and IAEA and was addressed to the General Assembly,[49] no such review has been conducted to trace the evolution of the United Nations International Computing Centre and critically examine its capacity and inherent potential to respond to the more contemporaneous needs of the system. Noting previous calls by JIU to uncover possible impediments in this regard, and without prejudice to the implementation of the formal recommendations contained in the present report, **the Inspectors envision that a comprehensive analysis of the United Nations International Computing Centre could be undertaken in the future, particularly with a view to determining the structural, financial and administrative conditions that would enable it to fully realize its potential as a strategic partner and resource for the United Nations system as a whole.** For the purposes of the present review, one of the questions that guided the Inspectors' examination of the United Nations International Computing Centre's offer of cybersecurity services in particular, as well as its set-up and vision for its own positioning in that specific field, was whether and to what extent the conditions were already present for it to become a cybersecurity hub for the United Nations system.

Mandate and business model

140. **Evolution of the United Nations International Computing Centre from 1971 to 2021.** Pursuant to General Assembly resolution 2741 (XXV), the United Nations International Computing Centre was established by a memorandum of agreement concluded in 1971 between the United Nations, UNDP and WHO. As an inter-organization facility originally created to provide "electronic data-processing services" for its three founding members and other users, its service catalogue and client base have evolved significantly since the 1970s. Best known for its hosting services and the shared ICT infrastructure it provides in support of the enterprise resource management systems of many of its clients, the United Nations International Computing Centre's scope of activity has expanded into areas as diverse as cloud computing, robotic process automation, blockchain, software development, ICT consulting and cybersecurity. Similarly, its client base has grown considerably. Conceived from the outset as a facility to be joined by additional clients, its clientele multiplied from the initial 3 to more than 25 United Nations system organizations by 2003 and some 70 clients in 2021, including entities of the United Nations family and affiliated organizations as well as several non-affiliated intergovernmental organizations, international NGOs and international financial institutions. Its constituent instrument was amended in 2003 to provide a broader legal basis and more detailed rules of engagement for its functioning, adding a newly formulated "mandate" document to concretize and expand the few basic provisions contained in the original document. It was

[49] A/8072.

separately adopted by all partner organizations through the United Nations International Computing Centre Management Committee and set out the Centre's governance structure, business model and basic conditions of participation. The United Nations International Computing Centre's two main functions, as reflected in that document, are to provide information technology services, including operational services and training, and to seek to ensure that the range of its services reflects the needs of its partner organizations.

141. **Basic tenets of the United Nations International Computing Centre's mandate and business model.** Through its updated terms of reference, the United Nations International Computing Centre reinforced the original purpose of its establishment as a service provider to the United Nations system organizations, closely tying its service offer to the concrete demand generated by its clients. At the same time, the reformulation of its main functions enabled it to be as unrestrained as possible in its quest to take up new lines of work beyond the restrictive scope of data processing, providing it, inter alia, with the liberty to offer cybersecurity services even without an express reference to such in its mandate. One element that was re-emphasized and further elaborated into the new document was the notion of a shared infrastructure and shared services, the aim of which was to achieve economies of scale for United Nations International Computing Centre clients. This is referred to as the United Nations International Computing Centre's shared services model, which enables it to lower the costs of its services in direct proportion to the increase in the number of clients subscribing to the respective service. In contrast, elements that have remained unchanged during the 50 years of the United Nations International Computing Centre's existence include: (a) its cost-recovery model, which effectively requires all of its products to be pre-financed by its clients on the basis of established needs and collective approval, without generating any surplus revenue nor any budgetary leeway for research and development activities; (b) the voluntary nature of its service catalogue, which organizations can opt to make use of in exchange for a fee, or choose not to, deciding on a service-by-service basis; and (c) its dependence on a "host organization" (WHO), to which the United Nations International Computing Centre remains administratively and legally attached, relying on the facilities, administrative capacity and regulatory framework it provides in order to be able to contract, recruit, appropriate funds and operate in practical terms.

142. **Complex governance structure reflects client-driven service provider role.** In order to ensure the relevance of its portfolio to the clients it serves, the Centre develops its service catalogue in close cooperation with representatives of its partner organizations through the United Nations International Computing Centre Management Committee. This 41-member body does not represent the full clientele the Centre serves, as a distinction is made between partner organizations and users of its services, together referred to as its clients.[50] Only the former are Management Committee members with voting rights who have a say in what lines of service the Centre is mandated to develop, and clients who are not also partner organizations (that is, those who are mere "users") can only subscribe to existing, already developed services. In addition, under the service-by-service opt-in model, not all Management Committee members are cybersecurity service clients and vice versa (annex VIII). This entails a theoretical risk of hindering the development or enhancement of such services for which some but not all United Nations system organizations may have a concrete need. With regard to cybersecurity services specifically, an informal advisory group was established in 2020 featuring the top three funding contributors to cybersecurity services (presently UNDP, UNHCR and FAO), for the purpose of keeping an eye on the service offer with regard to quality and relevance and identifying additional opportunities for shared solutions. The group has a direct communication channel with the United Nations International Computing Centre's Chief of Cybersecurity

[50] As per the 2003 amendment to the founding memorandum of agreement, the term "partner organization" means any organization of the United Nations system that utilizes the International Computing Centre services and has been accepted as a partner organization by the Management Committee, while the term "users" means those Governments, intergovernmental organizations other than partner organizations, NGOs and other governmental entities that have been accepted by the Director to utilize the services of the Centre.

Services, although the final say regarding service development still rests with the Management Committee. Overall, the governance architecture of the United Nations International Computing Centre was found to be complex, mirroring the multilayered nature of its current business model. The question of whether that architecture, in its current form, could absorb and appropriately fulfil a more prominent, even mandated role for the system without requiring some significant adjustments was not obvious to answer. Some challenges in this regard are explored in further detail in section D of the present chapter.

143. **Advantages and drawbacks of the United Nations International Computing Centre business model.** Once a particular service has been developed, all clients subscribing to that service pay a usage fee, which is determined and reviewed on a yearly basis by the Management Committee and is usually adjusted downward to reflect economies of scale as more clients sign up and decrease the cost of the respective service for all. In this regard, the strict cost-recovery model under which the United Nations International Computing Centre has operated since its inception has the advantage of ensuring a high degree of transparency in the costing of services, forces continuous coordination with clients, and keeps the scope of the service offer in check by requiring the closest possible alignment between what is really needed and what is developed and produced in response. A commercial, profit-driven interest can therefore be all but excluded, and this is one of the aspects that distinguish the United Nations International Computing Centre from other vendors. At the same time, there is no dedicated budget to sustain core executive and administrative functions,[51] meaning that such costs must be factored into the fees charged for services offered. Its business model, which combines the principles of cost recovery and shared services, has proven to be both an enabler and an obstacle for the realization of the Centre's vision to become a cybersecurity hub for the system. It has created a situation in which the United Nations International Computing Centre's service offer is dependent on clients providing seed funding to cover the costs of developing a new service to meet demand, while many can only afford to buy the service so developed once a critical mass of clients has already subscribed to it. This aspect has the potential to systematically disadvantage financially less powerful agencies, whose cybersecurity needs may differ from those of their peers with more budgetary leeway to pre-fund specific services.

Cybersecurity service catalogue

144. **The United Nations International Computing Centre as a key player in the United Nations cybersecurity landscape.** Over the past few years, the United Nations International Computing Centre has established itself as a key stakeholder and resource on cybersecurity for the United Nations system. As attested to by many of its clients, the Centre has accumulated considerable cybersecurity expertise and capacity and has gradually expanded its offer to include 13 specialized services in that area, commonly known under the brand name Common Secure (figure IX and annex VII). The services cover both dimensions of cybersecurity governance and operational aspects and are offered by the United Nations International Computing Centre in its capacity as: an infrastructure hosting provider that also manages security aspects of the data, systems and applications hosted; a dedicated cybersecurity service provider; an advisor on strategic and managerial questions; or a hands-on incident responder, depending on the type of services subscribed to. The versatility of the United Nations International Computing Centre's service offer on cybersecurity reflects the fact that this line of services has seen a significant growth in demand among its clients. Even though cybersecurity-related products represent only a fraction of the Centre's service catalogue and merely 6.1 per cent of its overall funding volume (as at January 2021), its (current and past) client base for such products comprises 45 organizations, 21 of which are CEB member organizations (out of a total of 31) and 20 of which are JIU participating organizations (out of a total of 28). Despite the fact that about one third of the respective organizations are not covered by United Nations International Computing Centre cybersecurity services, notably including the United Nations

[51] The United Nations International Computing Centre Director's report and financial statements for the biennium 2016–2017, published in April 2018, p. 46.

Secretariat, it is difficult to conceive of cybersecurity in the United Nations system today without considering the role and contribution of the Centre.

Figure IX
Overview of United Nations International Computing Centre cybersecurity services (2021)

Services	*Number of Joint Inspection Unit participating organizations (past and current clients)*
Common Secure Threat Intelligence	17
Common e-signature service	14
Incident response	11
Governance and chief information security officer support services	11
Information security awareness	10
Vulnerability management	7
Penetration testing	7
Phishing simulation services	6
Common security operations service	5
Cloud security assessment	5
Common public key infrastructure	3
Identity and access management	3
Common secure information and event management	1

145. **Common Secure Threat Intelligence as the United Nations International Computing Centre's flagship cybersecurity service.** Among the 13 cybersecurity services offered by the Centre, some have already attracted a considerable number of clients within the United Nations system and beyond, while others have yet to secure a client base. One particularly popular service, with 17 subscriptions from among participating organizations, has been the Centre's Common Secure Threat Intelligence, which can be considered to be its flagship cybersecurity service and attests to its utility. Common Secure Threat Intelligence has been assessed in particularly positive terms by a clear majority of the Centre's clients and addresses a long-standing collective need formulated and repeatedly reiterated at the system-level. The service combines various internal and external, including commercial and governmental, sources of threat intelligence, analysed and filtered by the United Nations International Computing Centre to produce digestible information packages tailored to the United Nations setting and audience. At a special session on cybersecurity in October 2020, the Centre's Management Committee approved a resolution requesting all partner organizations and clients to share threat intelligence and security incident information, in either attributable or anonymized forms, with the Common Secure team for analysis and sharing with the wider United Nations family. The Inspectors welcome this decision but note that, according to information received, it is yet to be implemented across the board. This area was one that most of the participating organizations surveyed by JIU found amenable to closer cooperation on a system-wide level, with some remarking that, in addition to sharing threat intelligence and, in particular, indicators of compromise, it would also be useful to exchange information on concrete response and recovery measures taken. The latter aspect, however, did not garner uniform support among the experts interviewed by the Inspectors, mainly due to confidentiality concerns. Nevertheless, Common Secure Threat Intelligence can be considered the most promising cybersecurity service in terms of its potential to naturally attain full system-wide subscription and realize actual protection gains for the system even beyond what it already achieves today. The same potential cannot be as easily ascribed to the entirety of the United Nations International Computing Centre's cybersecurity service portfolio.

146. **Assessment of United Nations International Computing Centre cybersecurity services is uneven.** Despite the close control that the United Nations International Computing Centre's clients have – in structural terms – over the services offered to them, the feedback from participating organizations regarding their satisfaction with said services was rather uneven, ranging from "very satisfied" to "very dissatisfied". This may be attributable to several factors. On the one hand, of the 20 participating organizations who subscribe or have in the past subscribed to at least one of the Centre's cybersecurity service, there is some variation as to how many and which services were subscribed to and therefore rated as satisfactory or not by each. The variation in the maturity of the respective organization's cybersecurity framework could also have affected the degree to which each was able to fully absorb and benefit from all aspects of the service offered. On the other hand, some of the services that are now listed separately used to be bundled together and offered as a package, which in itself had attracted some criticism due to the necessity for entities to subscribe to parts of the package that they did not need in order to avail of other, required or desired, parts. The United Nations International Computing Centre reportedly discontinued this practice in 2019 and now allows its clients full flexibility in choosing the level and type of service that suits them best. In addition, a basic satisfaction rating may convey a more general statement about the interaction or another aspect of the experience with the Centre that renders it less reliable and insufficiently nuanced to be conclusive. Given these limitations and the fact that it was not the Inspectors' aim to assess the effectiveness of each service or the United Nations International Computing Centre's service catalogue as a whole, it was not possible to discern an obvious pattern with regard to the type, size or maturity of those organizations that were more critical or supportive of the Centre than others. Overall, one can say that there are a number of organizations, large and small, that have been highly appreciative of the Centre as a cybersecurity provider, while equal numbers have taken a severely critical stance vis-à-vis the Centre. Such criticism may, in some cases, reflect historical shortcomings that might have been overtaken by subsequent developments and should therefore not obscure the present and future potential of the Centre as a cybersecurity service provider. However, reservations expressed could very well be contemporaneous, continuously valid or even recurrent over time and should thus be taken very seriously. In any case, regular and granular client satisfaction assessments can provide valuable insights into where the Centre may be well advised to apply greater efforts to respond to its clients' concerns and may in time attract additional clients. Moreover, a comprehensive assessment of the United Nations International Computing Centre as a cybersecurity service provider may be beneficial in providing more objective assurances of the overall quality and fitness-for-purpose of the Centre's line of services in this area.

147. **Perceived advantages of engaging the United Nations International Computing Centre.** Reasons to engage the United Nations International Computing Centre, as relayed by its clients, have included its intimate knowledge of the system and the needs of United Nations system organizations by virtue of its long-standing experience with the development of customized services for them, the fact that it is subject to the same administrative rules and structures, and its engagement with relevant inter-agency forums. In addition, the Centre has highlighted several comparative advantages that set it apart from commercial service providers, including: the progressive decrease in the cost of its services as its client base grows; the absence of profit-orientation and the associated interest to keep its prices affordable, including for less affluent organizations in search of low-cost options; the inherent and shared objective of rendering the system more secure for all, including for itself as a member of the family; and the ability to observe, adapt to and learn from its clients first-hand, scaling lessons learned directly for the benefit of the collective. The bird's eye view of the system as a whole and all its parts also distinguishes the United Nations International Computing Centre from commercial providers, who tend to see only parts of the larger puzzle, and thus ensures that it can add value beyond the individual context of any given client. Another aspect that the Inspectors found compelling was the notion that, despite existing inter-agency mechanisms and the added layer of representation-based governance of the Centre's Management Committee, there was no single entity that was intrinsically motivated to pursue the distinctly collective interest of the

system rather than its members' individual or, at most, cumulative – and often irreconcilable – interests. The United Nations International Computing Centre saw itself as a neutral, apolitical and – due to its cost-recovery model – disinterested broker of system-wide solutions in this regard, informed by the common good rather than some of the acute resource scarcity considerations that might guide the members of its Management Committee and entangle them in a potential conflict of interest.

148. **Perceived shortcomings of the United Nations International Computing Centre as a cybersecurity provider.** In contrast, several organizations have given a less laudatory assessment of the United Nations International Computing Centre as a cybersecurity service provider, specifically critiquing the aspect of its value for money in comparison with what commercial providers can offer. Some conveyed their impression that external companies were able to provide state-of-the-art expertise and tools at a level that exceeded the capacity that the United Nations International Computing Centre or any one organization could attain even after significant investments. Such impressions were countered by other voices among its clients who reported a veritable leap in expertise and cyberpreparedness on the part of the Centre in recent years, corroborated by evidence of significant investments by its leadership into ISO certification and compliance, diversified hiring of experts and the setting up of a shared security operations centre that operated non-stop, expanding the United Nations International Computing Centre's around-the-clock monitoring capabilities and enhancing its service catalogue. However, these efforts cannot distract from the fact that the perception persists of a continued gap in expertise and value for money that is – perhaps rightly – difficult for the Centre to overcome. It was further pointed out that similar services were available at a more competitive price from the private sector, and some respondents considered that, despite economies of scale related to the shared services model, the Centre charged too much for some of its services, and in an untransparent way, rendering them unaffordable or opaque to some and not sufficiently offset by gains in other areas to others. The United Nations International Computing Centre in fact acknowledged that competing with the private sector was beyond its capabilities and even counterproductive in some respects. Considering its business model, the cost of its services would generally be reduced if more clients joined, while the cost is, in many cases, the entry barrier for organizations wishing to sign up for the services in the first place. This paradox could be alleviated by, for example, injecting some less strictly tied funding in the right places, allowing the Centre to lower some of its fees, potentially below those of private sector providers, without having to attempt to replace them fully. Noting that it does not make sense to compete with the private sector in areas where it adds more value and is more efficient, executive heads should explore whether the United Nations International Computing Centre could act as an interface between commercial providers and their United Nations system clients in order to lower contractual fees and achieve economies of scale, and ultimately bargaining power. Moreover, and in conjunction with the independent assessment of its cybersecurity services suggested above, the United Nations International Computing Centre may wish to undertake a critical analysis of its cybersecurity service catalogue to better distinguish those services where the Centre may have a comparative advantage and consider investing more of its efforts in those areas. Ultimately, the Inspectors observed that, despite the sometimes harsh critique of the United Nations International Computing Centre as a cybersecurity service provider, the system makes use of its offer.

149. **Opportunities for improvements within the existing boundaries of the United Nations International Computing Centre's mandate.** While some organizations have advocated for a formal strengthening of the United Nations International Computing Centre's standing as a cybersecurity provider for the United Nations system, the Inspectors believe that a great deal can be accomplished within the framework of the Centre's current mandate as revised in 2003, which already provides a sound basis for the implementation of solutions that could come alive with a little more engagement of all stakeholders. Even if changes to its mandate were to become necessary for pertinent reasons, they lie within the collective competence of its founding organizations and those entities that signed on to the amendment of its constituent instrument in 2003 and would not require action by the General Assembly,

pending a more comprehensive analysis of the United Nations International Computing Centre as an entity, its accomplishments to date and possible structural reasons for its unrealized potential that could be addressed by such action. In the Inspectors' view, one key aspect to address without delay or further precondition would be to get to the bottom of and tackle the prevailing disconnect between existing structures and mechanisms and some constraints in the current funding pattern, as detailed below.

D. Improving linkages between system-wide strategic direction and operational capacity

Addressing the institutional disconnect between the Information Security Special Interest Group and the United Nations International Computing Centre

150. **Relationship between the Information Security Special Interest Group and the United Nations International Computing Centre formally limited.** Given the considerable overlap between the organizations represented in the inter-agency coordination mechanisms on the one hand and the United Nations International Computing Centre Management Committee on the other hand (annex VIII), one would assume that the Information Security Special Interest Group is the body that provides strategic guidance and direction on shared cybersecurity solutions that could be suitable for the United Nations system organizations, while the Centre functions as the operational implementation arm of the system. However, the two entities are not linked formally, nor are they operating jointly in practice. Formally, the Information Security Special Interest Group itself only exercises a coordinating and information-sharing role and is not mandated to instruct the United Nations International Computing Centre in any way, while the latter executes the decisions of its own Management Committee regarding the services to be developed for its partners and clients, which do not include all United Nations system organizations. In practice, the institutional disconnect between the two bodies may not be the decisive factor, but it is likely to have contributed to a dynamic that may be costing the system dearly in terms of efficiency gains due to missed opportunities for more direct collaboration.

151. **Strained interactions in practice owed to a series of factors.** As a matter of fact, the United Nations International Computing Centre has been granted observer status within the Information Security Special Interest Group and participates in the latter's discussions without a right to vote or to table items for debate. However, the Centre stated that it had effectively been denied the possibility of promoting its service catalogue in the Information Security Special Interest Group forum or of requesting direct feedback on its solutions in that setting. This stance may be explained in part by the nature of the United Nations International Computing Centre as an inter-organizational facility rather than an entity whose status could confer upon it CEB membership and thus full rights of participation. It was also suggested that there was an underlying perception that the United Nations International Computing Centre was primarily a vendor rather than a partner for the organizations of the system, which further hindered its full integration into existing inter-agency mechanisms. Considering its client-driven set-up and its role as a supplier of custom-made computing services for its partner organizations, it is hard to deny that the perception of being a vendor has some merit. At the same time, the Centre openly portrays itself as a United Nations entity and a full-fledged member of the United Nations family. In fact, its leadership has been vocal about its willingness to constitute the United Nations International Computing Centre as a cybersecurity hub for the United Nations system if given the opportunity to do so, while some organizations even opined that the Centre should make cybersecurity its core business. However, until challenges are addressed and resolved regarding the dynamics between the mandated inter-agency mechanisms for the system and the United Nations International Computing Centre as a privileged cybersecurity service provider with the potential to assume the role of the system's operational arm in this area, this scenario is likely to be destined to remain out of reach.

152. **De facto parallel structures.** One example that illustrates how the dynamic between the inter-agency mechanism and the United Nations International Computing Centre has prompted spontaneous solutions to identified needs but concomitantly created duplication in the area of cybersecurity is the case of the Common Secure Conference hosted by the Centre. Since 2019, the conference has provided a vehicle for the Centre's cybersecurity service clients to exchange information on matters of common interest at the operational level and provide feedback on the services provided. It has become a recurrent and well-regarded event on the cybersecurity calendar, generating a lot of praise from its attendees, many of which are United Nations system organizations that are also represented within the Information Security Special Interest Group. In a sense, the Common Secure Conference can be said to have filled a gap for the United Nations International Computing Centre, which sought to engage with the organizations through the Information Security Special Interest Group directly but was unable to do so in as productive and concrete terms as it would have wished with regard to its objective of improving its partnership with the system and operational aspects of its service offer. Some might even say that the conference has de facto become the leading forum for a large part of the system as a direct consequence of the inability of the existing coordination mechanism of the Information Security Special Interest Group to arrive at the operationalization of a more solution-oriented debate. The downside of these proactive and innovative developments is that the conference may have diverted some discussions that could well have been conducted within the Information Security Special Interest Group to another forum, which in theory is mainly open to clients of the United Nations International Computing Centre rather than the system as a whole. The existence of these two – in effect parallel rather than complementary – structures serving very similar purposes, one under the auspices of CEB and the other under those of the United Nations International Computing Centre, bears the risk of creating further disconnect and competition, resulting in ineffectiveness, duplication and overlap. This is one of the detrimental side effects produced by the unsatisfactory management of the dynamic between the two.

153. **More synergies needed.** These observations should inform the actions of both entities in attempting to improve the way in which they engage with each other. On the one hand, the Information Security Special Interest Group needs to step up its efforts as a collective to fulfil its mandate in a more strategic sense, identifying areas amenable to shared solutions, if not for the system as a whole, then at least for clusters of organizations whose improved cybersecurity posture would elevate that of the system. If it fails to do so, making use of the authoritative voice it holds on behalf of the system, chances are that the United Nations International Computing Centre will be forced to step in and occupy that space in a way that remains restricted to the circle of clients to whom it caters. At the same time, the United Nations International Computing Centre seizing the opportunity of the vacuum inadvertently created by the Information Security Special Interest Group is, in principle, beneficial for the system due to its innovative potential, but this should not happen in isolation from the official body in charge of system-wide cybersecurity coordination and cooperation. Both entities have a responsibility to proactively seek ways to improve the dynamic between them, whether through formal or informal measures. In fact, a number of well-subscribed cybersecurity services of the Centre are considered to have been inspired by or to have directly emanated from the exchanges carried out in the context of the Information Security Special Interest Group, even without having been commissioned by the latter in any formal sense. Especially if the United Nations International Computing Centre remains committed to continuing on its path to becoming a cybersecurity hub for the system rather than only for its own clients, it cannot afford to remain detached from the expert community representing the collective needs of the organizations that such a hub would serve. Moreover, the Information Security Special Interest Group, as a collective, holds part of the key to facilitating a more constructive collaboration in this regard. The potential for synergy and greater complementarity is there but has not been fully realized to date.

154. **Participating organizations to reconsider using United Nations International Computing Centre cybersecurity services.** As one way of addressing the prevailing disconnect between the two entities, some have suggested making usage of United Nations International Computing Centre cybersecurity services mandatory for United Nations system

organizations. This, it was argued, would also accelerate potential efficiency gains and cost reduction by reinforcing the scope and reach of the Centre as a shared service provider. This vision was not shared by all and may in fact be counterproductive. On the one hand, it would remove agency from the United Nations system organizations in evaluating and deciding on the service offer that best fits their needs by imposing and introducing an artificial monopolization of the provider and service offer externally. On the other hand, there are functioning governance mechanisms inside the United Nations International Computing Centre that already allow for a healthy exchange between its executive management and its clients around the shaping of cybersecurity services. The Inspectors consider it neither prudent nor necessary to interfere with these mechanisms. **However, already in 2019, the Inspectors encouraged the United Nations system organizations and the United Nations International Computing Centre to find more common ground to complement the existing capacities of the organizations with more shared services.**[52] In particular, the Inspectors believe that some of the reasons that may have led individual organizations to unsubscribe from or abstain from subscribing to the Centre's cybersecurity services in the past may be worth revisiting. The decision to do so will have to be a nuanced one, ideally (re)assessing each cybersecurity service offered on its own merit. Some of the services may indeed not yet have attained the level of maturity or be sufficiently responsive to organizations' needs for all members of the system to decide to subscribe to them. It is up to the United Nations International Computing Centre to continue its efforts to address any gaps in this regard. The Inspectors further recognize the individuality of each organization. It is ultimately the responsibility of the organizations to make relevant decisions based on their specific needs, notably taking into consideration the diversity of information systems, applications and other technical arrangements set up internally or framed in contractual arrangements with external providers.

Voluntary donor contributions to complement financing of shared solutions for the system

155. **Voluntary contributions as a means of direct support.** In the opinion of the Inspectors, it is timely to consider the use of voluntary contributions as a complementary funding mechanism to provide more direct resources for safeguarding the overall cybersecurity posture of the system. The availability of voluntary contributions earmarked for system-wide measures could remove some of the stumbling blocks hindering the implementation of shared cybersecurity solutions, as the lack of resources within participating organizations is likely to have impacted their readiness to contribute to a common pool of funding. Offering the system the possibility of tapping into a source of donor contributions that is independent from its members' individual budgets may relieve some of the pressure imposed, on the one hand, by the very limited leeway built into those budgets with so many corporate priorities competing for increasingly scarce funds and, on the other, by the United Nations International Computing Centre's cost-recovery model. In the case of the latter, it would permit the development of innovative service lines for its partner organizations, particularly those that rely on a less developed internal capacity or have fewer resources for setting up cybersecurity arrangements in general. In combination with its shared services model, such an approach would continue to contribute to cost efficiencies by keeping service charges low and would be likely to attract additional clients, thereby further multiplying positive effects. Whether the mechanism to collect and expend such voluntary contributions would be best placed under the direct authority of the system as a collective, for example as a trust fund to be set up under the administration of the CEB secretariat benefiting from the substantive input of the Information Security Special Interest Group, or with the United Nations International Computing Centre as the de facto established provider of many shared solutions for the system, was among the questions the Inspectors contemplated in consultation with relevant interlocutors. Having looked into various options in this regard, the Inspectors determined that the best place for such a fund would be

[52] JIU/REP/2019/5.

with the entity that would require operational visibility over expenditures on a day-to-day basis in developing the desired services, namely the United Nations International Computing Centre.

156. **Cybersecurity Trust Fund.** In principle, the United Nations International Computing Centre's mandate, since its amendment in 2003, includes provisions that enable it to collect voluntary contributions, and there has been a precedent of a specific project funded through this channel in the recent past. This mechanism has been underutilized to date, and its strategic employment for the proactive design of services to be shared among all or several United Nations system organizations has the capacity to become a game changer. Advertising the existence of this possibility more broadly and refining the conditions under which it can happen would provide an opportunity to Member States wishing to contribute directly to cybersecurity enhancement across the system, under the terms applicable to the respective earmarked contribution to support shared cybersecurity solutions. It would also facilitate the implementation of the 2019 JIU recommendation on a funding mechanism allowing the United Nations International Computing Centre to conduct research and development activities outside of the constraints of its cost-recovery model, which could further benefit its clients among the United Nations system organizations. The Inspectors therefore recommend that, following appropriate consultations, the Director of the United Nations International Computing Centre should establish a cybersecurity trust fund for the specific purpose of designing and developing the shared cybersecurity services that are most needed by the system. To further distinguish this mechanism from other sources of funding provided to the Centre by its partner organizations and clients, the creation of a dedicated trust fund would be prudent, with special conditions attached to ensure that its governance did not replicate existing structural biases, potential conflicts of interest or unhelpful dynamics emanating from the overlapping yet distinct membership of its Management Committee and that of the relevant system-wide inter-agency bodies.

157. **Operationalizing the trust fund.** Accordingly, the terms of reference of such a funding mechanism would be key to its success. These should clarify the roles and responsibilities of the different stakeholders, the types of services it is supposed to fund and the procedures for allocating funds in a transparent manner, including associated reporting requirements. In particular, the fund should be set up to be primarily used for purposes with tangible outputs for organizations of the system. The main aim of the fund could be to finance research and development for the purpose of launching cybersecurity services for which there is clear interest among organizations but no initial critical mass of users who are prepared to share the seed funding needed. Similarly, the fund could be used to extend the scope or depth of the existing services for which there is a clear demand and which require seed funding, or the cost of which would need to be lowered to enable more organizations to join sooner. While the trust fund would generally be subject to the WHO financial rules and regulations, under which the United Nations International Computing Centre operates, there is an opportunity to build into its governance an element of consultation with the competent inter-agency bodies. This would help to shape shared solutions to be developed for the system as a whole rather than only for the Centre's clients and would thereby further improve the utilization of resources available. Given its role in providing the basis for the creation of the United Nations International Computing Centre, the General Assembly is invited to take note of the recommendation to establish the cybersecurity trust fund and invite Member States to contribute to it.

158. The implementation of the following recommendations is expected to enhance coordination and cooperation among the United Nations system organizations.

Recommendation 3

The Director of the United Nations International Computing Centre should seek to establish by no later than the end of 2022 a trust fund for donor contributions, which would complement the capacity of the Centre to design, develop and offer shared services and solutions to enhance the cybersecurity posture of the United Nations system organizations.

Recommendation 4

The General Assembly of the United Nations should, no later than at its seventy-seventh session, take note of the recommendation addressed to the Director of the United Nations International Computing Centre to establish a trust fund for shared cybersecurity solutions and invite Member States wishing to reinforce the cybersecurity posture of the United Nations system organizations to contribute to the trust fund.

E. Opportunities for a closer alignment of physical security and cybersecurity

159. **Cybersecurity not covered in the United Nations security management system.** In its resolution 59/276, the General Assembly established the Department of Safety and Security with a system-wide mandate for setting a policy and accountability framework as well as operational standards and procedures for the safety and security of United Nations personnel and assets. Perhaps unsurprisingly, the mandate assigned to the Department of Safety and Security back in 2004, predating major system-wide developments in the area of cybersecurity in 2013 and 2014, did not contain any explicit reference to cybersecurity, nor did it contain references to the protection of data and digital assets or the cyberenvironment more broadly.[53] Even though the Department of Safety and Security indicated that information security guidance was applicable system-wide, the United Nations security management system and its associated policy documents had yet to articulate the points of convergence between physical security and cybersecurity for the purpose of determining the responsibilities of the various stakeholders of the system in that regard. The Inspectors welcome the fact that a placeholder heading entitled "Information security – sensitivity, classification and handling" has been introduced into the United Nations Security Management System Security Policy Manual, and they consider this to be a sign that there is some recognition of the relevance of cybersecurity considerations for the physical safety and security function. However, the related chapter is "yet to be developed", and the Department of Safety and Security expressed reservations regarding the need for such a separate chapter at this point in time. Meanwhile, as confirmed by the Office of Legal Affairs, and contrary to the settled interpretation that legal references to the protection of property and assets in the relevant conventions and host country agreements are understood to encompass digital assets and communications, neither the mandate nor the associated policy framework governing the physical safety and security function in the United Nations system can be said to cover cybersecurity today.

[53] The Department of Safety and Security indicated that the specific categories of security risks covered by the Department and the United Nations security management system were civil unrest, armed conflict, terrorism, crimes and hazards (non-deliberate).

160. **The Inter-Agency Security Management Network and the Information Security Special Interest Group.** The terms of reference of the Inter-Agency Security Management Network, which supports the High-level Committee on Management in its comprehensive review of policies and resource-related issues pertaining to the United Nations security management system and monitors the implementation of security management policies, practices and procedures by all actors of the United Nations system, also lack a specific reference to cybersecurity. Research conducted by JIU confirms that the Inter-Agency Security Management Network has only approached the topic on rare occasions and mainly from the perspective of the use of ICT to enhance the overall physical security processes, such as for identity and access management purposes (e.g. exploring options for biometric identification access cards for entry to physical premises as well as the digital space) or ICT-aided certification procedures for travel security clearances. More recently, a recommendation by the Information Security Special Interest Group on the establishment of coordination between the Group and the Inter-Agency Security Management Network "on issues of mutual interest" was adopted by the Digital and Technology Network in 2019.[54] However, the Inspectors could not find evidence that the stated intention had materialized beyond the context of specific projects. Relevant inter-agency mechanisms are invited to further explore the practical modalities of establishing a more regular channel of communication for increased collaboration. A suggestion made to the Inspectors in this regard was that the mutual participation of the Chairs of the Network and the Group in the meetings of both entities could facilitate the exchange of lessons learned.

161. **A blueprint for engagement with national authorities on cyberincidents.** One area where the procedures established for physical safety and security may provide some inspiration for the cyberrealm involves engagement with national authorities regarding cyberattacks. In chapter II (paras. 35–37) of the present review, the Inspectors covered in some detail the complex internal process leading to a decision on whether to contact national authorities, leaving aside the question of what would happen once such a decision was made and how communication with the respective governmental counterpart would unfold. The matter is far from straightforward, as the most appropriate counterpart at the national level may vary between the responsible ministry under which national computer emergency response (or readiness) teams, also known as computer security incident response teams, operate (e.g. ministries of internal affairs, defence, communication or technology, depending on the respective jurisdiction) and parallel capacities that may exist in the same State under the national intelligence agency with a mandate to pursue cyberattacks with a possible political dimension. Therefore, a central focal point may not automatically exist at the national level to formally receive relevant reports from United Nations system organizations, and this may complicate the appropriate channelling of information. By way of guidance for managing physical security-related crises, the United Nations Security Management System Security Policy Manual provides that designated officials "shall request the host Government to designate focal points with the authority to mobilize and coordinate support when a crisis affects the United Nations in the country".[55] An analogous approach could be explored as a blueprint for cyberincidents, acknowledging at the same time that designated officials would benefit from the expert advice of their corporate cybersecurity function on such matters.

162. **Absence of mechanism to transmit, receive and channel cyberrelated information within the system.** Similarly, internal arrangements for receiving cyberrelated information from Governments should be in place, yet these could not be readily discerned by the Inspectors in the course of their review. Some interlocutors implied that there was some confusion among governmental counterparts about which organization to contact when a cyberattack detected at national level revealed a link with one or more United Nations system organizations, and about what channel of communication to use. It was suggested that such intelligence was often

[54] CEB/2019/HLCM/DTN/02 and CEB/2019/HLCM/DTN/07, pp. 4–5.

[55] The United Nations Security Management System Security Policy Manual, sect. D – Relations with host countries on security issues, para. 14(d), "Crisis management".

available and ready to be shared but that no mechanism existed to reliably transmit and channel it to the intended recipients within the system, particularly as it was not obvious to external entities which member of the United Nations family the intelligence might pertain to. This in turn was said to have led in the past to missed opportunities to protect and defend organizational assets against intrusions, because it could not be ensured that such cyberintelligence would reach a recipient with the necessary expertise to render it actionable. The established diplomatic channels of communication were thus not considered to be sufficiently effective, leading to unrealized cybersecurity gains for individual organizations and for the system as a whole.

163. **Desirability and suitability of a harmonized approach.** Some of the factors leading to the current, uneven practice among the United Nations system organizations with regard to cooperation with national authorities are explained in paragraphs 35 to 37 above. The question arises as to whether related inconsistencies may create additional challenges, including potential reputational risks in managing host country relations, especially in cases where several United Nations organizations with divergent approaches to the matter are headquartered or maintain a presence in the same country, dealing – or not – with the same authorities on cybersecurity matters. **The Inspectors request the High-level Committee on Management to reflect collectively on the desirability and suitability of a harmonized approach to such cooperation and the development of corresponding guidance in this regard.** The Information Security Special Interest Group, the Inter-Agency Security Management Network and the Legal Advisors Network are well placed to lend their respective expertise to a joint examination of the matter and to look into potential security gains, associated challenges and, in particular, the feasibility of designating organizational focal points, including at the level of the system, to transmit, receive and channel information on cyberthreats and risks. Bearing in mind that the United Nations International Computing Centre participates in the Inter-Agency Security Management Network, the Inspectors noted that the Centre had expressed its readiness to play a role in consolidating and communicating information on cybersecurity incidents to national authorities on behalf of the United Nations system organizations, if formally entrusted with such a role. While reporting and cooperation with national authorities is a matter within each organization's own remit, the fact that the United Nations International Computing Centre has access to information that enables it to discern connections and potential interdependencies between attacks against different organizations that arguably none of the latter could put together on their own is an argument for a potentially increased role for the Centre in such matters and should be explored. In their consideration of a potentially harmonized approach in this regard, the relevant inter-agency mechanisms should therefore also invite and study the potential contributions of relevant stakeholders, including the United Nations International Computing Centre, particularly as concerns the latter's capacity to collect, correlate and analyse forensic evidence of cyberintrusions on behalf of the system.

164. **Towards closer alignment of physical security and cybersecurity.** More generally, and given that the 1992 guidelines on information security developed by the predecessor of the Digital and Technology Network already touched upon the links between the security of information systems and physical security,[56] and that the issue surfaced again in the discussions of the relevant bodies in 2013 and 2014,[57] the Inspectors consider it timely to revive efforts to establish a closer alignment of the physical security and cybersecurity functions to ensure the highest possible protection against complex threats. The Department of Safety and Security, as the central authority and standard-setting entity for the entire system, has a crucial role to play in acknowledging the existing convergence points and can become a key contributor towards a major shift in corporate culture. Indeed, in the United Nations system, threats to physical security are already taken extremely seriously, and there is no question about the need to

[56] Information System Security Guidelines for the United Nations Organizations.

[57] CEB/2013/5, para. 40; the nineteenth session of the Inter-Agency Security Management Network (2013, document without a symbol) and the twentieth session of the Inter-Agency Security Management Network (2014, document without a symbol).

address physical threats immediately and effectively. While the Inspectors detected a sense of cautious evolution of corporate thinking with regard to attaching the same sense of urgency to organizations' approach to cyberthreats, more needs to happen in order to extend the already prevailing risk-based approach and structured, accountability-centred response of the Department of Safety and Security from the purely physical realm to the cyberrealm. This is not to imply that the system-wide mandate already bestowed upon the Department of Safety and Security should be revised to absorb cybersecurity. The Inspectors acknowledge that dealing with the modern challenge posed by cyberthreat actors requires resources and specific expertise that the Department of Safety and Security does not have at present and that transferring any portion of responsibility for that matter would not be possible without significant adjustments. Any move in that direction would necessitate structural changes, including action by the General Assembly and extensive internal consultation and coordination with the various stakeholders of the United Nations security management system, including on aspects relating to administrative and financial resource requirements as well as the need to upskill security personnel, as argued elsewhere in the present report (para. 68). At present, the review shows that system-wide debate around this question is not mature and would benefit from renewed efforts and a closer examination, building on the expertise available in the system and notably at the level of the Inter-Agency Security Management Network and the Information Security Special Interest Group. The Inspectors therefore recommend that the Secretary-General explore opportunities to further draw upon the convergence between physical security and cybersecurity in the United Nations system and study the benefits and constraints of possible ways of doing so. A report to the General Assembly on the matter should, to the extent possible, be informed by the outcomes of consultations to be held between the relevant inter-agency coordination mechanisms seized with cybersecurity and the Inter-Agency Security Management Network, with input from the United Nations International Computing Centre as appropriate.

165. The implementation of the following recommendation is expected to enhance the effectiveness of the United Nations system response to cybersecurity threats.

Recommendation 5

The Secretary-General should present a report to the General Assembly of the United Nations no later than at its seventy-eighth session exploring further opportunities to draw upon the convergence between physical security and cybersecurity so as to ensure a more holistic protection of United Nations personnel and assets and indicating necessary measures to strengthen the existing structures accordingly, giving particular attention to the potential role of the Department of Safety and Security in this regard.

Annex I

Intergovernmental workstreams on cybersecurity and cybercrime

Introduction and terms used

Cybersecurity-related issues have been debated by the international community in several intergovernmental settings.

One the one hand, the topic has been examined by different committees of the General Assembly and bodies reporting to or otherwise associated with it. One workstream focused on cybercrime (referred to as computer-related crimes in the early 1990s), and the other on information and telecommunications in the context of international security (which includes ICT security and related subjects).

On the other hand, several participating organizations' mandates comprise aspects of cybersecurity that are subject to the intergovernmental processes supported by those organizations, for example ITU, the Office for Disarmament Affairs, UNODC, WIPO, UNDP, UNCTAD and IAEA.

The terms "cybercrime" and "cybersecurity" are not interchangeable, although they address the same issue from different angles. One could say that cybercrime focuses on the perpetration of cyberattacks and on the criminal responsibility of the attackers for their engagement in (cyberenabled or cyberdependent) illicit activities. In contrast, cybersecurity is concerned with defending against such attacks, putting the target and its defences rather than the perpetrator at the centre of attention.

The present annex provides an overview of the different intergovernmental workstreams at the level of United Nations system organizations, their origins and current work, as well as the relationship between them, where such exists.

Workstream I: cybercrime

Cybercrime on the global agenda since the 1990s. The first documented record of awareness among the international community of the need for dedicated attention to the cyberdimension of programmatic work, as well as for investment into nation States' ability to fend off cyberattacks (supported by technical assistance from relevant United Nations system organizations), dates back to 1990 and originally arose in the context of combating cross-border crime. Specifically, in its resolution 45/121, the General Assembly endorsed the recommendations of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders and, in particular, the resolution on computer-related crimes, in which States were called upon to intensify their efforts to combat computer-related abuses more effectively. Work on the subject continues under the heading "countering the use of information and communication technologies for criminal purposes"[1] in the Third Committee of the General Assembly (the Social, Humanitarian and Cultural Committee) and under the heading "cybercrime" in the context of the Commission on Crime Prevention and Criminal Justice (a functional commission of the Economic and Social Council). It is supported substantively and administratively by UNODC.

Ongoing work towards an international convention on cybercrime. Efforts to compile a "comprehensive study of the problem of cybercrime" have been pursued since 2010 in the context of an open-ended intergovernmental expert group (referred to as the "IEG on

[1] General Assembly resolutions 73/187, 74/247 and 75/539 and earlier resolutions 55/63 and 56/121.

cybercrime"), which was convened for that purpose under the auspices of the Commission on Crime Prevention and Criminal Justice.[2] The body of work produced as a result has gained momentum and matured into a separate endeavour to draw up a legally binding instrument on cybercrime. The process of drafting and negotiating that instrument is overseen by an ad hoc committee to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes (referred to as the "ad hoc committee"), which was established by the General Assembly in 2019 and started its work in 2020.[3] The eventual output of that process is to be addressed mainly to nation States as parties to the resulting convention. The legal framework it provides is predominantly intended to govern the treatment of individual offenders (cybercriminals) at the national level, thus having little direct bearing on the United Nations system organizations' approach to cybersecurity. Related endeavours are therefore of limited concern to the present review.

Workstream II: information and telecommunications in the context of international security

In a second stream of intergovernmental work, as from 1998, "the consideration of existing and potential threats in the field of information security" started featuring in resolutions of the General Assembly under the newly introduced and henceforth recurrent agenda item titled "developments in the field of information and telecommunications in the context of international security".[4] Two intergovernmental bodies operating under the First Committee (the Disarmament and International Security Committee) of the General Assembly have been seized with the topic: (a) the Group of Governmental Experts, a body composed of a limited number of experts nominated by the Secretary-General and serving in their personal capacity,[5] presently the sixth of its kind since the establishment of the first such Group in 2004;[6] and (b) the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (open to all United Nations Member States, established in 2018).[7] The main objectives of the two Groups are "to consider existing and potential threats in the sphere of information security and possible cooperative measures to address them"[8] and "to further develop the rules, norms and principles of responsible behaviour of States [listed in the resolution] and the ways for their implementation."[9] Both the Open-ended Working Group and the sixth Group of Governmental Experts completed their work and adopted consensus reports in March and May 2021 respectively.[10] The recently established new Open-ended Working Group on security of and in the use of information and communications technologies for the period 2021–2025 is expected to consider the work of its predecessor (which covered the period 2019–2020) and to convene for the first time in 2021.[11] The work of these bodies is supported substantively and administratively by the United Nations Office for Disarmament Affairs.

United Nations system organizations' mandates on cybersecurity

Several United Nations system organizations' substantive and technical cooperation mandates touch upon aspects of cybersecurity. One example is ITU, which, inter alia, hosts the annual forum of the World Summit on the Information Society, the main vehicle for the furtherance of the issue of ICT for development, and is the sole facilitator for World Summit on the

[2] General Assembly resolution 65/230.
[3] General Assembly resolution 74/247.
[4] See General Assembly resolution 53/70 and its succeeding resolutions, the latest one being resolution 75/240.
[5] See General Assembly resolution 58/32.
[6] See General Assembly resolution 73/226.
[7] See General Assembly resolution 73/27.
[8] See General Assembly resolution 58/32, para. 4.
[9] See General Assembly resolution 73/27.
[10] See A/75/816.
[11] See General Assembly resolution 75/240.

Information Society action line C5, "building confidence and security in the use of ICTs". In this role, ITU works with key stakeholders to help countries, inter alia, adopt national cybersecurity strategies, establish national incident response capabilities, deploy international security standards, protect children online and build capacity. Some of the work undertaken in the context of the World Summit on the Information Society has been referenced in General Assembly resolutions entitled "creation of a global culture of cybersecurity", elaborated in the Second Committee of the General Assembly (the Economic and Financial Committee).[12] Other organizations with mandates comprising a cybersecurity component include UNODC, WIPO, UNDP, UNCTAD, the Office for Disarmament Affairs and IAEA, as well as numerous others to varying degrees.

A compendium of the mandates and main activities of United Nations system organizations on cybersecurity and cybercrime compiled under the CEB framework was intended to sketch all the ways in which those organizations had been involved, within their respective mandates and focus, in the delivery of technical assistance and support to policy formulation in the area over the years. However, the compendium has remained an internal document that proved too monumental a task to finalize and update. It provides voluminous proof of the diversity and fragmentation of the United Nations system organizations' programmatic work on the subject. In this context, the necessity for the system to take a coordinated and consistent approach, bearing in mind the complementary nature of as well as a degree of overlap between the respective mandates of each organization, has been repeatedly stated by the High-level Committee on Programmes.[13]

[12] See General Assembly resolutions 57/239 and 64/211.

[13] See, for example, CEB/2010/HLCP-XX/CRP.7, para. 3; CEB/2010/6, paras. 38–43; CEB/2011/HLCP-XXII/CRP.6; and CEB/2014/6, paras. 42–49.

Annex II

Some elements of a risk-based approach to cybersecurity

In addition to formally adding cybersecurity to the corporate risk register or risk matrix of an organization, the Inspectors wish to highlight three aspects of a risk-based approach to cybersecurity that may accelerate the attainment of related benefits: (a) a tailored, systematic and adaptive approach to risk assessments; (b) a high-level strategic risk appetite and tolerance statement; (c) adequate opportunities for cybersecurity specialists to feed expertise into the risk management process; and (d) the employment of penetration testing as a risk management tool.

- **Tailored risk assessments**. Cybersecurity risk assessments must be tailored to fit the context in which an organization operates, with due consideration given to criteria such as its mandate, financial and personnel capacity, business model, the type of information held or owned, and organizational particularities, notably how cybersecurity incidents would affect the delivery of mandated tasks, including in decentralized settings or diverse field locations. Some participating organizations refer to industry standards in support of their risk assessment process, which can be considered a good practice, provided that the standards referred to are themselves selected on the basis of how well they fit the context of the organization concerned (paras. 59–64). In addition to tailoring risk assessments, the aspect of periodicity is to be highlighted, which not only facilitates a systematic approach but also ensures the framework's adaptability and, ideally, ad hoc responsiveness to an ever-evolving threat landscape that may not align with regular review cycles.
- **Risk appetite and tolerance statement.** One key component of a more strategic approach to cybersecurity risk management is the articulation of a risk appetite and tolerance statement, ideally with the involvement of legislative and governing bodies as well as the organization's executive management (paras. 53–54). The risk appetite and tolerance statement is most meaningfully built on the basis of a comprehensive and periodic cybersecurity risk assessment, covering all categories of cybersecurity threats, not only adversarial ones and not only those external to the organization (paras. 25–29), and gathering information both from the ICT department about the state of corporate information systems and known vulnerabilities and from business units in the spirit of a whole-of-organization approach. Determining the adequate risk appetite becomes of paramount importance when based on a carefully selected and designed set of meaningful cybersecurity metrics. It is an organization-specific process that will drive further management decisions, such as the establishment of an internal (as opposed to outsourced) corporate cybersecurity capacity; the resources allocated to it; the instruments and policy guidance included in the regulatory framework; and investment and incident response decisions in the event of escalation. At organizations like WIPO and IAEA, which manage particularly sensitive information, the risk appetite may be low by default. Previous exposure to significant cybersecurity incidents may also lower an organization's risk appetite but carries the risk of leading to overinvestment in cyberdefences that may in turn create a false sense of security.
- **Cybersecurity expertise feeding into risk management processes**. Providing adequate opportunities for cybersecurity expertise to inform corporate risk management processes may seem obvious but is far from the reality in many organizations. The format and periodicity of related input is not decisive, but a reliable (unimpeded and non-ad hoc) form of access for cybersecurity professionals to the driving forces of risk management within an organization is essential and should be instituted in a systematic way that ensures that critical cybersecurity considerations are reflected at the design, implementation and monitoring phases of the organizational risk management

framework. In some organizations, where such a position exists, the chief information security officer participates in or has been made a formal member of the corporate risk management committee. The feedback received on this arrangement was positive, and it may be worth establishing as a practice across organizations.

- **Penetration testing as a risk management tool.** Penetration testing (often abbreviated as "pen" testing) is an authorized simulation of a real-world attack targeting organizations' networks, systems and human resources, using tools and techniques typically employed by attackers with a view to identifying vulnerabilities in an organization's protections, assessing the effectiveness of mitigation measures in place, and testing response and recovery procedures. Penetration testing is mostly done by external contractors under rules designed to enable a tailored and effective assessment while minimizing the possibility of serious damage to organizations' assets and processes. Several participating organizations make use of this tool, in some cases engaging different (e.g. alternating) contractors over a period of time, ideally with diverse profiles, whose task is to attack the organization ("red team") and test the preparedness of the defence ("blue team"). One organization has taken the approach of joining the external contractor (simulating the attack) with the members of its security operations centre (defending against it), enabling real-time communication between the teams regarding the results and possible mitigating actions ("purple team"). Whether using one or several contractors, penetration testing is a demanding activity that requires solid preparation and careful selection of trustworthy expert assessors (posing as attackers), as there are real risks involved in allowing even temporary access to sensitive systems and information. However, it is a sophisticated and effective risk management tool that can be used to support business continuity planning and is a solid method of gaining quick insights into the cybersecurity posture of an organization from a variety of angles, highlighting loopholes in its overall defences or specific vulnerabilities in isolated areas, depending on the defined scope of the exercise.

Annex III

Main industry standards on cybersecurity referred to by Joint Inspection Unit participating organizations

ISO 27001 (International Organization for Standardization, 2005)[1]

Mainly used for audit and compliance purposes, ISO 27001 primarily focuses and provides guidance on what should be achieved with regard to technical areas of cybersecurity defences. The standard follows a general set of 14 controls aimed at integrating cybersecurity within an organization's business objectives and risk management practices. Its main control groups cover information security policies, asset management, access control, operations and communication security, incident management and compliance. Due to its characteristics, the framework appears to be best suited to reviewing and auditing cybersecurity measures in larger, well-resourced organizations.

The United States National Institute of Standards and Technology framework, 1901[2]

By defining an organization's objectives and priorities and by organizing appropriate actions, the United States National Institute of Standards and Technology provides flexible and adaptable guidance for understanding cybersecurity risks. In addition to its internal guidance, the framework, last updated in 2015, also includes references to other standards, guidance and practices, such as the Center for Internet Security Controls, the International Organization for Standardization international standards, the Control Objectives for Information and Related Technology and others. The National Institute of Standards and Technology action plan identifies five core functions (identify, protect, detect, respond and recover) and classifies information and decision flows into different levels within an organization. Due to its highly holistic approach, the standard appears to be particularly well suited to defining an organization's cybersecurity strategies and policies.

The Control Objectives for Information and Related Technology (Information Systems Audit and Control Association (ISACA), 1996)[3]

The Control Objectives for Information and Related Technology, an information technology governance and management framework, is based on best practices that help organizations to reach their objectives in the areas of compliance and risk management and to align their information technology strategy with their goals. Its approach follows the concept of capability levels with an emphasis on customizing services to the needs of an organization. Under this international standard, information security aspects are categorized as being part of the risk management and business service continuity and availability. In addition to its internal material, the Control Objectives for Information and Related Technology references other standards and guides, including the United States National Institute of Standards and Technology framework, ISO 27001 and the Center for Internet Security Controls. The most relevant alignment goals contained in the Objectives include information technology risk management, information security, compliance, and business service continuity and availability. In terms of cybersecurity guidance, the standard appears to be particularly well suited for organizations that already make use of the Control Objectives for Information and Related Technology for their ICT governance and management framework. Furthermore, the criterion can be extended by combining it with other standards to which it refers (the Center for Internet Security Controls, the National Institute of Standards and Technology framework and ISO 27001).

[1] Available at www.iso.org/home.html.
[2] Available at www.nist.gov.
[3] Available at www.isaca.org/credentialing/cobit/cobit-foundation.

The Information Technology Infrastructure Library (Central Computer and Telecommunications Agency of the United Kingdom of Great Britain and Northern Ireland, 1980s)[4]

The Information Technology Infrastructure Library is a set of guidelines in ICT service management and comprises a series of publications providing relevant guidance on ICT services delivery and on the necessary processes and resources required by organizations. Developed by the Central Computer and Telecommunications Agency of the United Kingdom during the 1980s, the standard is presented as a series of five volumes, each covering a different phase of the ICT service management cycle. Key topics include service value definition, business development, service assets, market analysis and service provider types. As from 2005, Information Technology Infrastructure Library practices contributed to and aligned with the ISO 20000 standard.

Center for Internet Security Controls, 2008[5]

Also known as Critical Cybersecurity Controls, the standard provides a set of recommendations based on industry best practices. Although its orientation is primarily technical, the Center for Internet Security Controls also include a few controls dealing with broader organizational aspects of cybersecurity, such as awareness training and incident response. The framework appears to be quite practical and very useful in terms of implementation groups, focusing on actions to implement in accordance with an organization's size, skills, available resources and data sensitivity. Its main controls include inventory and assets, vulnerability management, secure configuration, email and web browser protections, data recovery and protection, incident response, and penetration tests. Such an approach has proven to be especially well suited to implementing cybersecurity defence strategies in small and medium-sized organizations with already existing risk frameworks that include cybersecurity aspects.

[4] Available at www.axelos.com/best-practice-solutions/itil.
[5] Available at www.cisecurity.org/controls/.

Annex IV

United Nations system organizations' regulatory frameworks on cybersecurity

(a) Layers of a cybersecurity regulatory framework

Strategic level	Often a single document containing high-level statements formulated in aspirational terms	Defines organizational vision, objectives and overarching principles, outlines basic governance and organizational roles and responsibilities, and may articulate cybersecurity as a business decision, including a statement on the organization's risk tolerance or appetite	Applies to the organization at the entity level, mainly addressed to senior management for implementation
Policy level	A series of stand-alone documents containing prescriptive, actionable language, usually published as official administrative issuances	Articulates organizational principles that underpin the Information Security Management System with binding internal regulations and rules containing statements of purpose and associated actions organized by topic (e.g. information classification, risk management, business continuity and disaster recovery, and acceptable use of ICT data and assets) and assign specific roles and responsibilities	Applies to all staff and implies the possibility of disciplinary sanctions in cases of non-compliance
Procedural level	A series of guidelines or standard operating procedures supporting higher-level policies by describing processes aimed at establishing systematic practices	Provides detailed guidance on specific steps to take or behaviours to avoid (adhering to password use conventions, running regular antivirus scans and software updates, scanning Universal Series Bus (USB) sticks received as giveaways before use; etc.)	May apply to all personnel or be geared towards specific roles (e.g. ICT staff, archive and records managers, and procurement specialists)
Technical level	A series of technical protocols aimed at correct and uniform execution	Outlines granular, step-by-step guidance requiring significant subject-matter know-how to apply and implement. Topics may include, inter alia, database configuration, network security and cloud security	Mainly addressed to technical experts

Source: Prepared by JIU.

(b) Information and communications technology strategies and dedicated cybersecurity policy documents in participating organizations

Participating organization	*Information and communications technology corporate strategy with a cybersecurity component*	*Dedicated cybersecurity policy documents*
United Nations Secretariat	Yes, Information and communications technology in the United Nations (A/69/517) and General Assembly resolution 69/262)	Yes, Information Security Policy Directive for the United Nations Secretariat (2013)
UNAIDS	No, ICT Strategy (2017–2020) does not include cybersecurity	No, UNAIDS is working on a global cybersecurity plan that will also include a cybersecurity policy
UNCTAD	Follows United Nations Secretariat Information and Communications Technology Strategy	Yes, follows United Nations Secretariat Cybersecurity Strategy
UNDP	Yes, Information Technology Strategy (2020–2023)	Yes, Information Security Policy (2016)
UNEP	Follows United Nations Secretariat Information and Communications Technology Strategy	Yes, follows United Nations Secretariat Cybersecurity Strategy
UNFPA	Yes, Information and Communications Technology Strategy (2018–2021)	Yes, Information and Communications Technology Security Policy
UN-Habitat	Follows United Nations Secretariat Information and Communications Technology Strategy	Yes, follows United Nations Secretariat Cybersecurity Strategy
UNHCR	Yes, Information Technology Strategy (2020–2022) (final draft under review)	Currently under development
UNICEF	Yes, Information and Communication Technologies Strategy	Yes, UNICEF Information Security Strategic Plan (2018–2022)
UNODC/UNOV	Follows United Nations Secretariat Information and Communications Technology Strategy	Yes, follows United Nations Secretariat Cybersecurity Strategy
UNOPS	A five-year ICT strategy (under development)	Yes, Information Security
UNRWA	Yes, Information Management Department Strategy (2019–2020)	There is a separate information security policy (pending final approval)
UN-Women	Yes, Information and Communication Technologies Strategy (2018–2021)	Yes, Information Security Policy
WFP	Yes, Corporate Information Technology Strategy (2016–2020)	Yes, Corporate Information and Information Technology Security Policy (2015)
FAO	Yes, Information and Communication Technologies Digital Strategy (2017)	Yes, Information Security Policy
IAEA	Yes, Business Technology Strategic Plan (2015–2020)	Yes, Standards on Information Security

Participating organization	*Information and communications technology corporate strategy with a cybersecurity component*	*Dedicated cybersecurity policy documents*
ICAO	Yes, Information and Communication Technologies Digital Strategy (2017) (under review)	Yes, Information Security Policy (2007, Rev. 2)
ILO	Yes, Information Technology Strategy (2018–2021)	Yes, Electronic Information Security, Policy Statements (2010)
IMO	Yes, Information and Communication Technologies Strategic Plan (2019–2023)	Yes, Information Security Risk Management (2015)
ITU	No, ITU has a more holistic approach with the introduction of an organizational resilience management system, including development of a detailed business impact analysis mapping strategic risks and business impact strategies, as well as crisis management, business continuity and ICT disaster recovery	No
UNESCO	Yes, Knowledge Management and Information and Communication Technologies Strategy (2018–2021)	Yes, included in enterprise risk management framework and the Administrative Manual (Information and Information Technology Security Policy)
UNIDO	Corporate Information and Communication Technologies Strategy (2029–2021)	No
UNWTO	No, Information and Communication Technologies Strategy does not include cybersecurity	No, under development
UPU	No, UPU ICT strategy will be available in December 2021	No
WHO	Yes, Information Management and Technology Strategy (2019)	Yes, Cybersecurity Strategy
WIPO	Yes, Information and Communication Technologies Strategy (new strategy under development)	Yes, Information Security Polices and Standards and Next Generation Information Security Strategy (2021–2024)
WMO	Yes, Information and Communication Technology Strategy (2020–2023)	No

Annex V

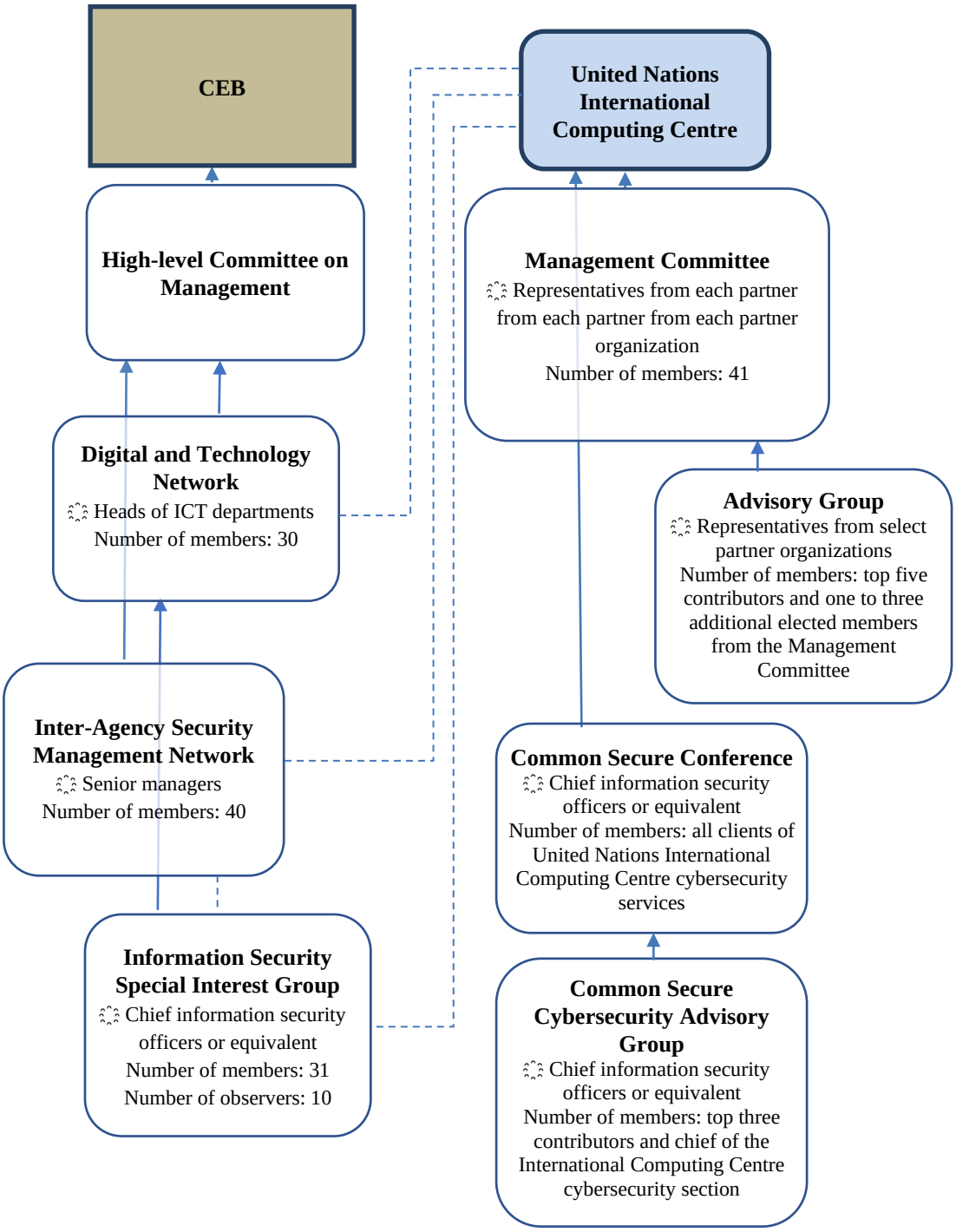
Cybersecurity arrangements and reporting lines in Joint Inspection Unit participating organizations as at January 2021

Participating organization	*Cybersecurity matters are managed by dedicated or specialized in-house capacity*	*Cybersecurity is covered by the corporate ICT department (among other ICT functions)*	*Used the "chief information security officer as a service" or security governance service provided by the United Nations International Computing Centre*	*Reporting line to Head of ICT (or equivalent)*
United Nations Secretariat	√		X	√
UNAIDS		√	X	√
UNCTAD		√	√ (Current client)	√
UNDP	√		X	√
UNEP		√	X	√
UNFPA	√ (Chief information security officer under recruitment)	√ (Until recruitment is completed)	√ (Current client)	√
UNHCR	√		X	√
UNICEF	√		√ (Current client)	√
UNODC/UNOV		√	X	√
UNOPS	√		X	Chief information security officer reports to Chief Finance Officer and Director of Administration
UNRWA	√		X	√
UN-Women		√	√ (Past client)	√
WFP	√		√ (Past client)	√
FAO	√		√ (Current client)	√
IAEA	√		X	√
ICAO	√		√ (Past client)	Chief information security officer reports directly to Head of Administration

Participating organization	*Cybersecurity matters are managed by dedicated or specialized in-house capacity*	*Cybersecurity is covered by the corporate ICT department (among other ICT functions)*	*Used the "chief information security officer as a service" or security governance service provided by the United Nations International Computing Centre*	*Reporting line to Head of ICT (or equivalent)*
ILO	√		X	√
IMO		√	X	√
ITU	√		X	√
UNESCO	√		√ (Current client)	√
UNIDO		√	X	√
UNWTO		√	X	√
UPU		√	X	√
WHO	√		√ (Past client)	√
WIPO	√		X	A combined chief security officer role responsible for physical security and information security, the Head of the Security and Information Assurance Division reports to the Assistant Director General for Administration, Finance and Management
WMO		√	√ (Current client)	√

Annex VI

Inter-agency institutional and operational arrangements regarding cybersecurity



Source: Prepared by JIU.

Annex VII

Overview of United Nations International Computing Centre cybersecurity services subscribed to by Joint Inspection Unit participating organizations as at January 2021

Cybersecurity service	*Brief description*	*Number of current Joint Inspection Unit participating organizations subscribing*	*Number of past Joint Inspection Unit participating organizations subscribed or completed projects*
Common Secure Threat Intelligence	Continuous and timely information gathering from agency members; commercial security firms; service providers; federal, state and local government agencies; law enforcement and other trusted resources, which enables entities subscribing to share any relevant and actionable physical security and cybersecurity threat as well as any incident information.	17	
Common e-Signature service	Offers the ability to provide digital signatures.	14	
Information security awareness	Offers strategic advisory services to help an organization set up a state-of-the-art, effective information security awareness strategy, an industry leading cloud-based learning lab or communications support, including deliverables with messages, bulletins, posters and portal support.	7	3
Vulnerability management	Combination of processes and technologies providing continuous identification and remediation of vulnerabilities and configuration flaws. This is achieved through, inter alia, host and application vulnerability scans, security configuration checks and Internet footprint monitoring.	6	1
Governance and chief information security officer support services	Information Security Management System service with the goal of protecting organizational assets and mitigating the risk of exposure to negative reputational impact, loss of relevant information and malicious acts as well as risks to intellectual property, sensitive data and reputation.	6	5

Cybersecurity service	*Brief description*	*Number of current Joint Inspection Unit participating organizations subscribing*	*Number of past Joint Inspection Unit participating organizations subscribed or completed projects*
Phishing simulation services	Tests the effectiveness of organizations' information security awareness programmes. The tool includes both the design and execution of phishing simulation campaigns and follow-up reports.	6	
Common security operations centre service	Provides specialized expertise to monitor, analyse and respond to cybersecurity events, enabling subscribing entities to respond to security incidents in a timely manner using a combination of technology processes and solutions.	4	1
Incident response	Provides incident handling procedures based on industry standards for analysing incident-related data and for determining appropriate responses to any organizational security incident in real time.	4	7
Cloud security assessment	Assessment, migration, implementation and fully managed operational support as well as cost management for a number of cloud solutions.	4	1
Penetration testing	Enables the identification of weaknesses in information security controls and determines the extent to which adversaries can penetrate the network or systems being tested.	3	4
Common public key infrastructure	Public and private key encryption and digital signatures are provided and managed, creating a secure environment for electronic transactions and data transfers.	3	
Identity and access management	Information on identity and access-management applications is gathered, analysed and presented.	2	1
Common security information and event management	Provides real-time analysis of security alerts generated by applications and network hardware.	1	

Source: The United Nations International Computing Centre catalogue of services (July 2021) and responses from participating organizations to the JIU questionnaires.

Annex VIII

Comparison of the membership of entities active in cybersecurity as at January 2021

Participating organizations	*Digital and Technology Network (Thirty-third session, 2019)*	*Information Security Special Interest Group (Eighth Symposium, 2019)*	*United Nations International Computing Centre Management Committee (2020)*	*United Nations International Computing Centre cybersecurity service clients (past and current)*
United Nations Secretariat	√	√	√	X
UNAIDS	√	X	√	X
UNCTAD	√	X	√	√
UNDP	√	√	√	√
UNEP	√	X	√	X
UNFPA	√	√	√	√
UN-Habitat	√	X	X[1]	X
UNHCR	√	√	√	√
UNICEF	√	√	√	√
UNODC/UNOV	X	X	X[2]	√
UNOPS	√	X	√	√
UNRWA	√	X	√	√
UN-Women	√	√	√	√
WFP	√	√	√	√
FAO	√	X	√	√
IAEA	√	√	√	√
ICAO	√	X	√	√
ILO	√	√	√	√
IMO	√	X	√	√
ITU	√	√	√	√
UNESCO	√	X	√	√
UNIDO	√	√	√	√
UNWTO	X	√	X	√
UPU	X	√	√	X

[1] The United Nations International Computing Centre communicated that UN-Habitat was represented on the Management Committee through the United Nations Secretariat.

[2] The United Nations International Computing Centre communicated that UNODC/the United Nations Office at Vienna was represented on the Management Committee through the United Nations Secretariat.

Participating organizations	*Digital and Technology Network (Thirty-third session, 2019)*	*Information Security Special Interest Group (Eighth Symposium, 2019)*	*United Nations International Computing Centre Management Committee (2020)*	*United Nations International Computing Centre cybersecurity service clients (past and current)*
WHO	X	√	√	√
WIPO	√	√	√	√
WMO	√	√	√	√

Annex IX

Glossary of cybersecurity-related terms

Bot herding, botnet	A botnet is a large number of compromised computers that are used to create and send spam or viruses or flood a network with messages as a denial of service attack. *Source*: ESCAL Institute of Advanced Technologies, glossary of security terms www.sans.org/security-resources/glossary-of-terms/
Compromise	The intentional or unintentional disclosure of information, which adversely impacts its confidentiality, integrity or availability. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Distributed Denial of Service attack	An attack in which multiple compromised systems are used to attack a single target. The flood of incoming messages to the target system forces it to shut down and denies service to legitimate users. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Encryption	A mathematical function that protects information by making it unreadable by everyone except those with the key to decode it. *Source*: National Cyber Security Centre (the United Kingdom) www.ncsc.gov.uk/information/ncsc-glossary
End point device	Any network connected device, such as desktop computers, laptops, smartphones, tablets, printer or other specialized hardware like point-of-sale terminals or retail kiosks, that act as a user end point in a distributed network. *Source*: Barracuda Networks Inc., Glossary www.barracuda.com/glossary/endpoint-device
Firewall	A security barrier placed between two networks that controls the amount and kinds of traffic that may pass between the two. This protects local system resources from being accessed from the outside. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Internet of things	The network of everyday web-enabled devices that are capable of connecting and exchanging information between each other. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Malware	Malicious software designed to infiltrate or damage a computer system without the owner's consent. Common forms of malware include computer viruses, worms, Trojans, spyware and adware. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary

Phishing	An attempt by a third party to solicit confidential information from an individual, group or organization by mimicking or spoofing a specific, usually well-known brand, usually for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information, which they may then use to commit fraudulent acts. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Ransomware	A type of malware that denies a user access to a system or data until a sum of money is paid. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Shadow IT	The use of hardware or software by a department or individual without the knowledge of the information technology or security group within the organization. *Source*: Cisco www.cisco.com/c/en/us/products/security/what-is-shadow-it.html
Social engineering	Manipulating people into carrying out specific actions or divulging information that is of use to an attacker. *Source*: National Cyber Security Centre (the United Kingdom) www.ncsc.gov.uk/information/ncsc-glossary
Spear phishing	The use of spoofed emails to persuade people within an organization to reveal their usernames or passwords. Unlike phishing, which involves mass mailing, spear phishing is small-scale and well targeted. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Spoofing	Faking the sending address of a transmission to gain illegal entry into a secure system. *Source*: Committee on National Security Systems (the United States) https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
Virtual private network	A private communications network usually used within a company, or by several different companies or organizations, to communicate over a wider network. Virtual private network communications are typically encrypted or encoded to protect the traffic from other users on the public network carrying the virtual private network. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary
Vulnerability	A flaw or weakness in the design or implementation of an information system or its environment that could be exploited to adversely affect an organization’s assets or operations. *Source*: Canadian Centre for Cybersecurity https://cyber.gc.ca/en/glossary

Annex X

Overview of action to be taken by the participating organizations on the recommendations of the Joint Inspection Unit

		United Nations, its funds and programmes																*Specialized agencies and IAEA*												
	Intended impact	*UNICC*	*United Nations*	*UNAIDS*	*UNCTAD*	*ITC*	*UNDP*	*UNEP*	*UNFPA*	*UN-Habitat*	*UNHCR*	*UNICEF*	*UNODC*	*UNOPS*	*UNRWA*	*UN-Women*	*WFP*	*FAO*	*IAEA*	*ICAO*	*ILO*	*IMO*	*ITU*	*UNESCO*	*UNIDO*	*UNWTO*	*UPU*	*WHO*	*WIPO*	*WMO*
Report: For action		☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒
Report: For information		☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐
Recommendation 1	**f**		**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**	**E**
Recommendation 2	**f**		**L**	**L**			**L**	**L**	**L**			**L**		**L**		**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**	**L**
Recommendation 3	**c**	**E**																												
Recommendation 4	**c**		**L**																											
Recommendation 5	**f**		**E**																											

Legend:

L: Recommendation for decision by legislative organ

E: Recommendation for action by executive head

☐ **:** Recommendation does not require action by this organization

Intended impact: a: enhanced transparency and accountability; **b:** dissemination of good/best practices; **c:** enhanced coordination and cooperation; **d:** strengthened coherence and harmonization; **e:** enhanced control and compliance; **f:** enhanced effectiveness; **g:** significant financial savings; **h:** enhanced efficiency; **i:** other.