Vision Paper
on the
UNICC Cybersecurity Fund (CSF)
for the United Nations System

April 2024

Vision Paper on the
UNICC Cybersecurity Fund (CSF) for the United Nations System

In 2021, the Joint Inspection Unit (JIU), the only independent external oversight body of the United Nations (UN) system, reviewed cybersecurity practices across the UN system and issued its report "Cybersecurity in the United Nations system organizations" (JIU/REP/2021/3). Two of the report's five recommendations pertain directly to UNICC and its role as the primary shared cybersecurity service provider of the UN system.

The JIU recommended

(1) that the UNICC Director establish a fund for voluntary donor contributions to "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", and

(2) that the UN General Assembly (UNGA) take note of the fund and invite "Member States wishing to reinforce the cybersecurity posture of the United Nations system organizations" to contribute to it.

In 2022 UNICC created the Cybersecurity Fund (CSF) as part of its commitment to honour the findings and recommendations contained in the JIU's report.

In December 2023, in a Resolution that addressed the JIU report on Cybersecurity, the General Assembly noted "with appreciation the report of the Joint Inspection Unit on cybersecurity in the United Nations system organizations, and [requested] the Secretary General and invites the executive heads of the member organizations, as appropriate, to implement the relevant recommendations" (A/RES/78/243).

The present Note sets out the basic tenets of the UNICC Director's vision for the future operationalization of the UNICC Cybersecurity Fund (CSF) for the United Nations system. It highlights the unique position and value-added UNICC offers and concretizes the opportunities and cybersecurity needs of the UN system that will be addressed through the CSF.

I. THE ISSUE

"Weak protection against cyberthreats in one organization makes the whole system more vulnerable." (JIU, 2021)*

The risk of the weakest link. In its report on Cybersecurity in the United Nations system organizations (JIU/REP/2021/3), the JIU uncovered the risks inherent in the interlinked nature of the UN system. It emphasized that "an organization with vulnerable or weak defences represent[s] a risk for the other entities of the system". Inspectors spoke of a "collective problem", finding that "the United Nations system is as strong as its weakest link". Over the past several years, UNICC has itself observed a consistent increase in the sophistication of attacks targeting the UN system, including by advanced threat actors and through active coordination of attacks across multiple UN entities at once. The challenge now transcends beyond any one organization and its critical information.

** Wherever quotation marks are used throughout the present Note, the referenced text represents a direct quote from JIU/2021/3.*

Why Member States should care. In the event of a successful cyber-attack, UN assets and the Member State data they hold are both compromised. Sturdy protection is thus both a mutual interest and a shared responsibility. The more sensitive the dataset, the more defences are needed. But protecting only the organization with the most sensitive data misses the mark. By exploiting the weakest links in the system, cyberthreat actors can infiltrate one organization and move laterally to the next from within, bypassing even the most elaborate outward defences of any given entity. Organizations, as well as Member States entrusting their data to them, therefore cannot afford to build their protections in isolation.

Cyber-resilience across the UN system cannot be effectively achieved when approached within organizational silos. When agencies work alone, protection is uneven, and exploitable gaps are created. This is the situation today. Should the UN system remain without a baseline level of cybersecurity across all UN entities, the risk of breaches and loss of data will remain as high in the best equipped entities as it is in the least equipped ones. A breach in one agency must be communicated across the system within hours – not days, weeks, or months. This is part of what UNICC already provides to its partner organizations under its flagship Common Secure service. However, too many UN system organizations are as yet unable to benefit from such shared services, with cost being one of the key entry barriers.

Silos create duplication, inefficiency, and donor funding "lock-in". When governments provide individual agencies with budgets for siloed cybersecurity capacity development, efforts are often duplicated unnecessarily across the system and serve to undermine system-wide endeavours. Individual solutions are built disjointedly for several organizations in parallel, even though shared solutions are either readily available or could be developed. Precious resources are committed to efforts that may serve only one single agency and are not shared across the system, which allows system-wide vulnerabilities and inefficiencies to persist. Allocating finite resources disparately also reduces the funding pool available to support solutions that benefit the entire system along with each of its members. Government funds end up scattered and "locked in" across multiple budgets when they could instead be deployed directly at source, benefitting multiple agencies with just one pledge to a shared service provider.

Vital need for a baseline system-wide cybersecurity posture. Securing a single UN entity without ensuring a baseline cybersecurity posture among interconnected entities is costly, inefficient and – most critically – provides a false sense of security. Investments into cyber-defences tend to reflect an organization's protection needs. However, from the point of view of an attacker, it is immaterial whose protection needs (in other words, the sensitivity of digital assets) and investments are highest – exploitation will happen wherever the guard is down. There is thus a vital need to develop a baseline defence for the UN system to prevent and mitigate against attacks, protecting UN and Member States data and digital assets in the most comprehensive way possible.

Complement rather than compete. The UNICC Cybersecurity Fund (CSF) will provide a dedicated stream of funding toward critical cybersecurity functions with the capacity to strengthen the UN System's cybersecurity posture at all levels – from HQs, to regional offices, to the smallest country outposts. By supplying funds to the CSF, governments will enable UNICC to further complement rather than compete with the work of other UN entities and mechanism already engaged in cybersecurity activities through its focus on shared services, fill gaps where needed in a quicker and more agile manner, incentivize agencies to invest more in cybersecurity due to the cost savings reaped by shared solutions, and promote a more concerted, coherent, and coordinated approach to cybersecurity across the system.

UNICC's expertise and operational capabilities, coupled with a dedicated funding stream for system-wide shared solutions, is currently the best available avenue to address the risks associated with organizational cyber-silos and to present a united, system-wide cybersecurity front.

II. WHY A CYBERSECURITY FUND FOR THE UNITED NATIONS SYSTEM?

The main mechanisms and vehicles supporting cybersecurity in the UN context have **two key structural flaws**, as identified by the JIU, which hinder the full realization of the potential that exists for shared solutions for the UN system:

(1) the **lack of any operational capacity and funding** associated with existing inter-agency mechanisms to implement solutions that the collective determines to be needed and worth pursuing for the benefit of all; and

(2) the funding constraints imposed on UNICC, which has the requisite capacity to implement, but is restricted by its **cost recovery model**, requiring its partners to fully pre-fund any solutions to be built, the cost of which many cannot afford upfront.

> *In the JIU's words:*
>
> *"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."*

The JIU recommended a dedicated fund for cybersecurity to sit with UNICC as the established de facto primary shared cybersecurity service provider of the UN system – and for good reason. UNICC has the technical expertise and operational capacity to raise the bar for the entire system to reach a common, baseline cybersecurity posture by mainstreaming core cybersecurity service offerings across the system while simultaneously consolidating existing efforts and creating economies of scale.

What UNICC needs to bring this vision to fruition is a **complementary funding mechanism** outside of its cost-recovery model that will allow it to put the full range of its know-how, and repository of tools and experience, to proactive use for the common good of the UN system. This is precisely what the JIU recommended and what UNICC has set out to provide a vehicle for.

Without a dedicated, independent funding stream for shared solutions benefitting the UN system, neither the prevailing inter-agency coordinating mechanisms on cybersecurity (DTN/UNISSIG) nor UNICC can make the leap from mere coordination and exchange of ideas on one side and strict cost-recovery with full pre-financing of each solution on the other, to proactively filling the gaps in existing solutions. **A new funding vehicle is necessary to provide entity-impartial support where the current cyber-defence landscape of the UN system is most vulnerable, acting solely with the system's collective interest**, rather than with individual organizational priorities, in mind.

Inaction ultimately risks stagnation in the UN system's cybersecurity preparedness in the face of one of the most dynamic and fastest-evolving threat landscapes facing the world today.

III. WHY UNICC?

UN's longest-standing strategic technological entity with a consistently growing portfolio and partners. Since its creation in 1971 pursuant to UNGA resolution 2741 (XXV), UNICC has grown from an inter-organization facility originally providing electronic data-processing services to its founding members – the United Nations, UNDP and WHO – to a strategic technological partner for the entire UN system and related multilateral organizations, offering shared digital solutions to more than 90 organizations tailored to the needs and requirements of UN agencies and entities.

UNICC acts as the *de facto* cybersecurity centre and shared service provider of UN cybersecurity with unparalleled expertise across the UN system. Today, UNICC is de facto the primary provider of shared cybersecurity services to UN system organizations. As a member entity of the UN family, UNICC is intimately familiar with the needs and requirements of the system and manages a cybersecurity service catalogue of over two dozen cybersecurity services used by more than 60 UN organizations, agencies, and entities. Furthermore, its shared services model translates to lower costs for each client with every additional subscription to its services. UNICC has experienced a 500% increase in the consumption of its cybersecurity services over the past 4 years, yielding significant economies of scale, naturally promoting a coordinated and needs-based approach to its service offerings, and contributing to the coherence, consistency, and complementarity of its services to augment existing capacities and efforts within its client and partner organizations. **UNICC currently has – by a tenfold margin – more cybersecurity experts than any other UN agency or entity of the system.** With over 200 cybersecurity practitioners focusing on building, implementing, and managing cybersecurity solutions and over 50 years of experience as a key strategic technology partner to UN system organizations, UNICC already functions as a hub for cybersecurity expertise and operational capacity to deliver solutions to shared challenges within the UN system.

In the JIU's words: "it is difficult to conceive of cybersecurity in the United Nations system today without considering the role and contribution of the Centre" (para. 144).

Optimally protecting the multilateral system and its parts. UNICC enjoys the same international protections as its founding organizations under the respective Conventions on the Privileges and Immunities of the United Nations (1946) and the Specialized Agencies (1947). By extending the same to the data, systems, and infrastructures it hosts, UNICC is uniquely positioned to protect the collective cybersecurity interests and needs of the system as well as its constituent parts in a way that no other UN agency or entity can on its own.

IV. WHAT COULD BE DONE FOR THE SYSTEM?

UNICC already collaborates closely both with UN system organizations individually, as well as with the prevailing inter-agency mechanisms on cybersecurity in the UN system, joining meetings as an observer and continuously taking the pulse of its partner organizations' needs through the latter's seat on the UNICC Management Committee. **UNICC therefore sees and experiences first-hand where the pain points of the system lie and what its most urgent cybersecurity needs are from a technical expert's point of view.**

UNICC sees **four areas of solution development that could be initiated in the immediate term** to benefit the system directly, but that are currently out of reach for lack of a more non-restrictive funding mechanism:

A) System-wide sharing of threat intelligence
B) System-wide cyberthreat prevention, detection, response and recovery capabilities (UN System-wide CERT)
C) System-wide data protection measures
D) Research and development (R&D) to secure the future

A) System-wide sharing of cyber threat intelligence (Common Secure for all)

UN agencies are regularly experiencing interrelated cybersecurity attacks and engaging in similar modes of response. From a single agency's limited perspective, some of the more complex and advanced threats may appear to be unique, but they are often linked to other threats occurring simultaneously across the system. Most often, individual agencies are not equipped to recognize such patterns, but UNICC's existing cybersecurity threat intelligence service, Common Secure, is precisely designed to do so. When a threat to one UN agency emerges, UNICC can and does provide advance warning to agencies not yet affected, strengthening the entire system's cybersecurity response as a result. Although approximately 60 UN entities have already signed up for this service, a significant portion still do not benefit. The Cybersecurity Fund would enable UNICC to lower the cost of this service to a point where no UN entity would experience any cost-related entry barrier, and UNICC could expand its protective shield to encompass the system as a whole. Recent discussions in relevant inter-agency fora have revealed an urgent need for optimally protected secure communication channels for sharing threat intelligence. A shared solution to share threat intelligence within the UN system has multiple benefits yet cannot be effectively and swiftly initiated without dedicated financial support to complement UNICC's traditional funding sources. UNICC's unique profile and cybersecurity capabilities, including its ongoing work on a UNICC Private Cloud, could translate this identified need into an operational reality for the UN system.

B) System-wide cyber threat prevention, detection, response & recovery capabilities (UN System CERT)

UN agencies and funds continue to experience a significant increase in cyber threats, with UNICC Cybersecurity detecting a 500% increase in cyberattacks on the UN system from 2021-2023.

Coordinating the implementation of uniform cybersecurity measures to strengthen the cybersecurity posture of the entire UN system can and will reduce the real and potential adverse impacts of these cyber threats. It will also enhance the UN system's ability to effectively and

uniformly detect, respond and recover from cyber incidents. Through the CSF, UNICC will augment its ability to provide expertise, capacity and recommendations to facilitate collaboration and coordination of a system-wide response to cyber threats experienced by all UN entities. UNICC currently offers a range of cybersecurity services to its partners, yet the adoption of these services is non-uniform and ultimately dependent on the availability of funding for each individual agency. With a common approach, UNICC can make all its cybersecurity services available to the entire UN system in an affordable, efficient and effective manner, thereby raising the cybersecurity posture of the entire UN system.

C) System-wide data protection measures

Today, no single United Nations organization can function without processing personal data, also known as Personally Identifiable Information (PII). With the ongoing digital transformation and rapid adoption of new technologies, the volume of collected PII has mushroomed, while the global average cost of a data breach has grown to over 4.45 million USD. Quite aside from cost implications, mishandling of PII can be harmful to both the operations and beneficiaries of the United Nations system organizations. In particular, beneficiary data is held and processed by UN agencies with varying levels of cybersecurity maturity and disparate controls to ensure their protection. Given the inherent intersection and overlap between cybersecurity and data protection measures, UNICC has established a structured approach to implement the technical aspects of data protection. Supported and further enabled by the CSF, UNICC will be empowered to implement this approach across the UN system, including through greater standardization of reporting data breaches and the process for managing such breaches consistently.

D) R&D for proactive cyber protection to secure the future

With the growing adoption of artificial intelligence within the UN system, and the looming post-quantum future on the horizon, an appropriate level of investment in state-of-the-art cybersecurity technology is indispensable for the UN to respond to next-generation threats proactively. The UN system needs to prepare itself for a post-quantum era in which the defenses of today will be rendered ineffective to the threats emerging in the future. As the JIU inspectors note, one "main aim of the fund could be to finance research and development", providing a vehicle to understand and counteract emergent cybersecurity threats and devising an early response to related needs. This can only be achieved by overcoming the limitations imposed on UNICC by its existing cost-recovery business model. Investing in cutting-edge R&D is necessary to stay ahead of the curve and ensure that the UN system can benefit from the development of solutions that will lead to effective mitigation measures before novel cybersecurity threats fully materialize.

V. GOVERNANCE

"…a cybersecurity fund for the specific purpose of designing and developing the shared cybersecurity services that are most needed by the system." (JIU, 2021)

In line with the JIU's recommendations, **UNICC aims to devise and establish a governance mechanism for the Cybersecurity Fund that will allow UNICC to identify and respond to the most pressing collective needs of the UN system organizations** by leveraging UNICC's long-standing experience, unique position and expertise, and proven internal governance mechanisms to build solutions in direct response to client needs.

> The JIU set out some key parameters for the Fund's terms of reference, namely:
>
> - "to support shared cybersecurity solutions" and "tangible outputs for organizations of the system"
> - "to extend the scope and 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";
> - "to finance research and development (R&D) 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";
> - "to distinguish this mechanism from other sources of funding provided to the Centre by its partner organizations and clients"
> - "to provide an opportunity to Member States wishing to contribute directly to cybersecurity enhancement across the system".

In 2022 UNICC put in place a distinct account ready to receive voluntary contributions from governments separately from any other funding streams.

An initial CSF Governance Committee comprised of representatives from UNICC's own governance structure, including the UNICC Management Committee Chair, and from donors, will ensure an **accountable mechanism of governance that is responsive to the UN system's needs** and to aid UNICC's decision-making regarding where and how to deploy the resources entrusted to it. UNICC also proposes to:

1. Earmark all voluntary **contributions exclusively for the design, development, deployment, and support of shared cybersecurity solutions** for the benefit of UN system organizations.
2. Conduct a **biennial consultation process** with UN system organizations, under the auspices of the UNICC Management Committee, to determine and validate the contemporary cybersecurity needs of the UN system.
3. Follow standard financial rules, regulations, accounting principles and reporting requirements as set by UNICC's administering host organization WHO and guided by UNICC's own Mandate and Management Committee.

VI. FINANCING

Contributions will be voluntary and initially limited to governments. Initially, private sector funding will neither be sought nor accepted in order to avoid any possible conflict-of-interest situations given UNICC's established cooperation with and track record in leveraging the services and know-how offered by leading private sector providers for the UN system. In the future, funding from the private sector, or other potential contributors such as academic institutions or philanthropic foundations, may be considered subject to parameters to be developed and agreed for this purpose in the context of the Fund's governing mechanism and guided by relevant organizational policies.

The **viability** of the Fund will depend on the first tranche of pledges and contributions from Founding Donors. However, long-term financial sustainability will be necessary to ensure that critical cybersecurity investments remain a priority. In the future, we anticipate 3-5 year replenishment cycles; however, for the sake of simplicity and expediency, the CSF will initially be set up with a 2-year funding goal.

A preliminary funding target of 30MM USD will enable UNICC to realize concrete and measurable system-wide cybersecurity gains. More detailed funding needs, as well as necessary adjustments to the terms of reference, if any, will be determined once (a) the governance structure is in place, and (b) the initial funding target has been reached.

Staffing costs for the day-to-day management of the Fund and its associated consultative governance mechanism remain to be determined, but may include a fund manager position, a technical (cybersecurity) advisor, and support staff.

VII.NEXT STEPS AND AREAS FOR CONSULTATION

As UNICC works to further concretize its vision for the operationalization of the Cybersecurity Fund, the organization welcomes observations, responses, additional questions, or any other feedback on the present paper and the vision for the UNICC Cybersecurity Fund for the United Nations system.

UNICC

Palais des Nations
1211 Geneva 10
Switzerland
www.unicc.org