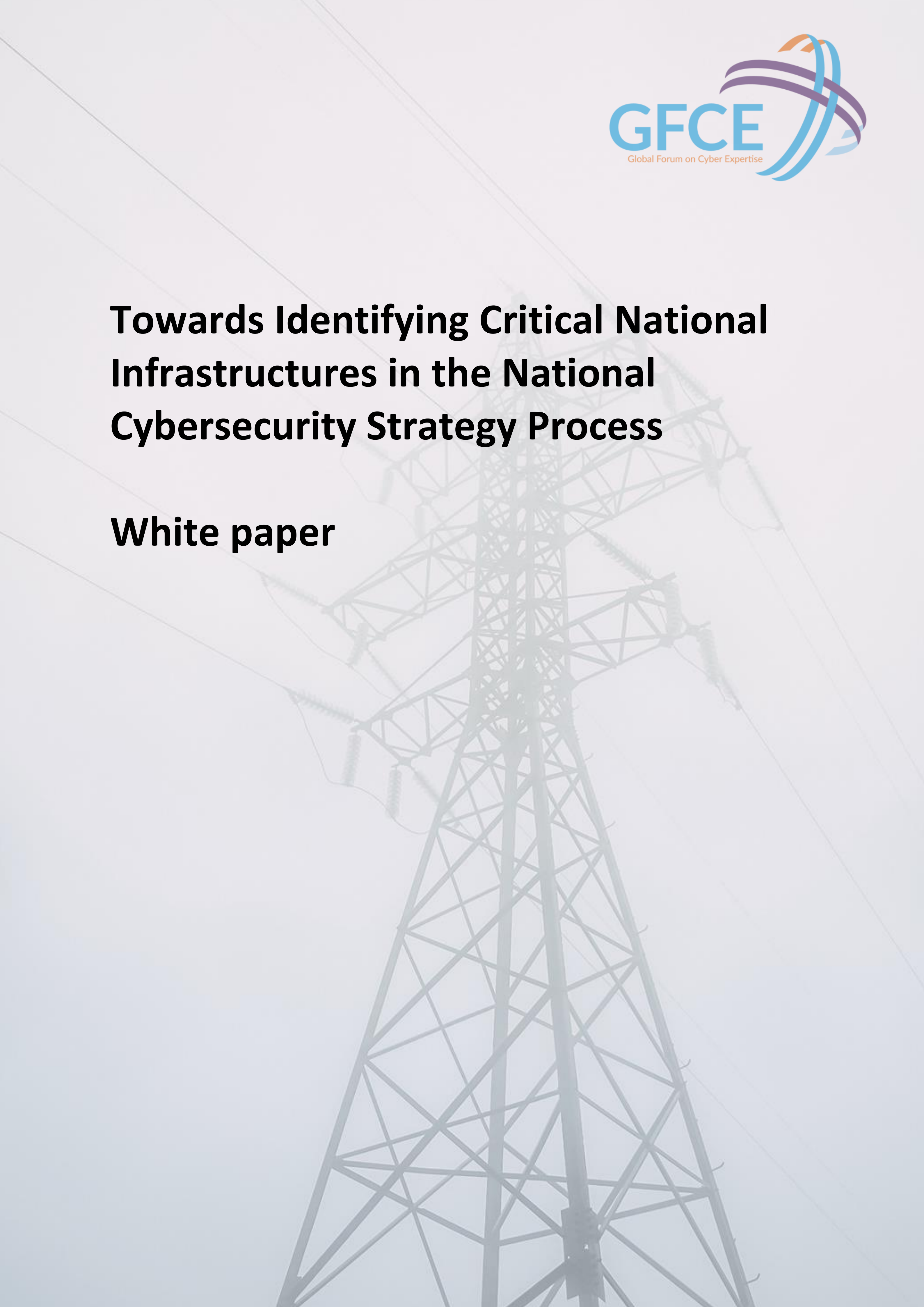
GFCE
Global Forum on Cyber Expertise



Towards Identifying Critical National Infrastructures in the National Cybersecurity Strategy Process

White paper

Thanks and contributions

This white paper was developed in 2021 by the GFCE’s Working Group B Cyber Incident Management and Critical Infrastructure Protection and the Working Group A Task Force Strategy & Assessments (S&A). The contributors include Abdul-Hakeem Ajijola, Giacomo Assenza, Marwan Ben Rached, James Boorman, Enrico Calandro, Rick Harris, Marc Henauer, Tadas Jakštas, Orhan Osmani, Andy Purdy, Roxana Radu, Milan Sekuloski, Carmen Valeria Solis Rivera, Ian Wallace and Carolin Weisser Harris.

The Working Group B and Working Group A Task Force S&A would like to thank César Moliné Rodríguez, Kathleen Bei and Velimir Radicevic for their support realizing this white paper.

The cover image is attributed to MusicFox Fx on Unsplash.

Disclaimer

The information and views set out in this paper are those of the authors and do not necessarily reflect the official opinion of the GFCE, its Secretariat or its members and partners. Neither the GFCE nor its members may be held responsible for the use which may be made of the information contained within.

Background

In 2021, the Task Force Strategy & Assessments (TF SA) of the Global Forum on Cyber Expertise (GFCE) developed a *"Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle"* (GFCE, 2021) to help countries to understand and plan the different steps in the National Cybersecurity Strategy process. One important activity elaborated in the *Catalog* is advice on methods for identifying Critical National Infrastructure (CNI)[1]. In order to understand CNI/Critical Information Infrastructure (CII) risks and determine risk mitigation measures, nations must formally identify critical infrastructure in a systematic, contextualized way that informs CNI/CII protection and risk governance approaches. To date, there is no standard methodology to help nations address this foundational identification task. This white paper builds upon existing CNI/CII work within the GFCE and proposes some practical considerations and measures for how countries can develop approaches for identifying CNI/CII as part of their NCS development and implementation processes.

The white paper addresses three foundational elements related to CNI/CII identification in the context of NCS development. A fourth section identifies areas where additional research is needed.

- Section I addresses potential approaches for identifying the ICT risk aspects of CNI/CII;
- Section II discusses potential approaches for formalizing the identification of CNI/CII in NCS and/or law and ways to build a national consensus around the need to protect the most important ICT assets;
- Section III identifies a range of potential governance structures for implementing CNI/CII portion as part of NCS implementation;
- Section IV identifies CNI/CII protection research needs.

Section I – Perspectives on Identifying the ICT Risks of CNI/CII as part of the NCS Process

Every NCS should address how the nation intends to identify CNI/CII and the measures it takes to increase resilience. National strategies may integrate or update existing CNI/CII policy guidance, legal frameworks, or national programs that address critical infrastructure, or they may establish those policies if none exist. When developing policies and strategies to identify CNI/CII, policymakers may consider the following perspectives.

[1] This white paper uses the term Critical National Infrastructure (CNI) to describe, broadly, physical and virtual infrastructure that supports vital national functions as well as national goals and aspirations. For the purposes of this paper, critical information infrastructure (CII) is an important component of CNI, especially to the extent different national functions rely on information and communications technology (ICT) for their operation. The authors recognize that all CNI increasingly relies on ICT and therefore are increasingly subject to ICT risks. Additionally, the emergence of cyber/physical risks and potential life-threatening consequences of cyber/physical disruptions is making CII risks almost indistinguishable from overall CNI risks. Consequently, the paper refers to the broader category of CNI/CII as the objective area for national risk identification and mitigation efforts.

Transnational Perspective: NCS strategy developers addressing CNI/CII should have an understanding of related international policies, norms, and best practices. They should also explore the CNI/CII identification approaches of other nations to better situate and contextualize the effects of relevant practices. Additionally, NCS strategists should understand the implications of CNI/CII across sectors and borders considering dependencies and interdependencies between different jurisdictions including mapping supply chains.

Societal Perspective: A key part of the NCS process needs to address the potential societal harms associated with the disruption of essential functions supported by critical infrastructure, e.g. loss of trust within society or civil disorder when critical services such as healthcare, education, and food supply are interrupted or pose a risk to economic viability. Thinking in terms of how critical service disruptions could impact citizen may uncover perspectives on risks associated with services that have not traditionally been prioritized. The COVID-19 pandemic has provided a stark reminder of the need to maintain a high level of resilience for essential services that have been moved online (CyberPeace Institute, 2021). Such an assessment is dependent on:

- a clear determination of the reliance of critical infrastructure functions on ICT networks and systems, particularly operational technology (OT) environments;
- a clear determination of the roles and responsibilities of public authorities and private operators in the identification of critical infrastructure, in fully public, fully private or hybrid set-ups.

The identification of ICT risks should also take into account the level of cyber risk awareness among the population. The perception of risk may vary from one context to another, but the overall preparedness of a country also depends on the importance that citizens place on risk mitigation measures. The expectations set for critical infrastructure owner and operator roles should be known to citizens and become part of a public deliberation. For instance, citizens and communities that have significant experience dealing with frequent disruptions to critical services from government or CNI/CII owners and operators may have developed resilient local capabilities to compensate for these disruptions. Efforts to increase resiliency of national infrastructure should consider the potential impacts on existing local resiliency measures. Additionally, while critical infrastructure owners and operators as well as citizens ultimately desire a rapid return of services after their disruption, governmental concerns over criminal investigations or needs to respond to national security concerns may delay the return of critical infrastructure to full operations. It is important that all stakeholders be aware of different aspects of cyber risks and resiliency in CNI/CII.

Another aspect to consider is identifying the current 'risk tolerance' of a society, i.e., consider how resilient a society is currently to CNI/CII disruptions through local and community mitigations. For instance, citizens may have some tolerance for the lack of electricity because of existing weaknesses in infrastructure and cyber risks may not be a significant aspect of those disruptions or their impact. On the other hand, the disruption of distribution of some government services (food, healthcare, loan programs, etc.) may be less tolerated by citizens and need addressing from a cybersecurity standpoint by government. An assessment of 'risk tolerance' may inform national mitigation priorities and approaches.

Section II – Considerations for Formalizing the Identification of CNI/CII and Building Stakeholder Consensus

This section provides a discussion of factors to consider as nations develop and 'formalize' processes of identifying CNI/CII and designate or create organizations to coordinate those processes. Formalizing the ways and means of identifying CNI/CII may generally require:

- Developing an NCS and including an implementation plan for identifying CNI/CII;

- Designating or creating a governance body to coordinate identification processes;

- Determining relevant governmental authorities, roles, and responsibilities, as well as technical and policy capabilities among public and private critical infrastructure stakeholders; and

- Gaining broad consensus agreement on an identification process for CNI/CII.

While this section does not attempt to address every conceivable approach to formalizing the identification of CNI/CII, it intends to help generate future studies and analysis that will help nations choose the best way, under their national circumstances, to identify and address critical infrastructure. The diversity of national governments, economies, national security circumstances, societies, and cultures challenge any single approach to identify the "best practices" for identifying critical infrastructure and it is very likely that the economic and political development of a country, or public/private relations, or other social and political factors would have a significant bearing on how a nation formalizes critical infrastructure identification, and vastly different approaches may result.

Nations may apply different frames of reference as they work to identify CNI/CII. Many, such as in the case of the U.S., initially oriented CNI/CII efforts around discrete sectors such as the financial service, energy, or transportation sectors, to identify and address critical ICT assets. This approach has been modified over time to focus more on identifying critical national functions which is intended to facilitate cross-sector views of risk vs. within single sectors and helps account for the possibilities of cascading effects when critical assets are disrupted. Nations with less extensive infrastructure environments may have a frame of reference that orients on critical assets vs. critical functions, especially if a sector, such as the energy sector, consists of a small number of providers. Approaching the identification of CNI/CII from an asset-based, sector-based, or functional perspective depends on national circumstances; however, each of these aspects must be understood to fully address CNI/CII identification and mitigation programs.

There are several foundational considerations when formalizing national processes and organizations to identify CNI/CII such as identifying and following national mandates; exploring intergovernmental organizational approaches; and establishing CNI/CII identification criteria. In the case of n*ational mandates, for instance,* policymakers should first consider their national constitutions and legal frameworks. This may be an obvious point; however, identifying and formalizing CNI/CII protection requires the participation of the whole of society and must be consistent with the existing legal frameworks to ensure that institutional roles and responsibilities are appropriately aligned. Also, in many cases, national constitutions may provide explicit or implied mandates to protect designated CNI/CII and, by implication, the CII that supports those functions. This is especially the case when identifying and protecting CNI/CII intersects with national security considerations and the constitutional mandates of the government to ensure national sovereignty; establish parameters for national defense; ensure continuity of government and the economy; as well as protect and keep its citizens safe. National constitutions also establish the form of national government and governance processes that should be leveraged to shape how formal CNI/CII is characterized and determined. Also, to be sustainable, formal processes for identifying CNI/CII should conform to constitutionally mandated governmental roles and responsibilities, especially regarding the relationships between government and the private sector.

National laws (“ordinary” law derived from a constitution) and implementing policies, as well as national-level economic and security strategies are usually developed by legislators, heads of state, and government organizations to address the practical aspects of governing a nation. When considering CNI/CII identification governance and processes, policymakers should first inventory existing laws, policies, and national strategies. Existing policies, especially those that provide for the physical security of critical assets such as national communications systems, may also be critical sectors, functions, or assets that rely on information technology and are more subject to CII risks. If this is the case, some government organizations may already be assigned to assure their security. Consideration should be given to including CII risk management as another component of physical risks in these circumstances. Additionally, sectors and assets that are currently regulated or in some cases, State-Owned Enterprises (SOE), may already meet a country’s definition of criticality from a physical perspective and should be evaluated for the degree of their exposure to cyber risks as well. Some examples may include communications infrastructure that is essential for continuity of government; prioritized transportation infrastructure that supports disaster relief efforts; or healthcare facilities that support pandemic responses.

While developing critical infrastructure identification processes, nations should also consider their obligations under international treaties and voluntary international agreements. Some examples include agreements to ensure the protection of infrastructure related to maritime trade, collaboration to counter cybercrime under Budapest Convention on Cybercrime (Council of Europe, 2021) or the adoption of voluntary norms such as the United Nations’ Group of Governmental Experts (GGE) Framework for Responsible State Behavior in Cyberspace (United Nations, 2021).

Section III – Potential Governance Structures for CNI/CII

A national government's structure for dealing with CNI/CII should be clearly identified in a declarative policy, ideally within a NCS that is developed through a multi-stakeholder/consensus process. Additionally, developing implementing policies that mandate intergovernmental cooperation to protect CNI/CII is essential. Even if a government has already addressed physical risks to critical infrastructure and tasked certain government organizations with mitigating those risks, there may not be coordination between them. Therefore, policies that mandate cooperation and information sharing between governmental organizations as well as governmental policies, platforms, and mechanisms that facilitate these mandates are essential.

General 'good practices' for a governmental group or organization tasked by an NCS, or other policy to formalize processes for CNI/CII identification may include:

- The group has sufficient legal authorities and mandates to coordinate across government and with critical infrastructure owners and operators;

- The group reports directly to the head of state or Head of Government who is also responsible for the national defense;

- The group ensures equal voices in identifying critical infrastructure among civilian and national security government organizations, and critical infrastructure owners and operators;

- The group contains technical and policy-level competence in multiple potential critical infrastructure sector domains (i.e., energy production and distribution; finance; communications; etc.);

- The group includes private sector membership or a strong mechanism for private sector input.

Establishing a CNI/CII identification governance process must start somewhere and usually requires an explicit implementation directive from national leadership. For instance, the Head of Government may designate an organization or a task force/group to evaluate and recommend different CNI/CII approaches. This same task force/group, or a different group or organization, may be tasked with implementing the government's decision.

Governments may consider establishing a commission consisting of private and public stakeholders to develop a CNI/CII strategy and recommendations on how the nation should organize to formalize CNI/CII identification. Such a commission should consist of policy and technical experts in likely critical infrastructure domains, as well as elements of government that have roles and responsibilities in prospective CNI/CII sectors such as regulators, national security organizations, and standards bodies. The commission should also include major private sector entities or have a means for ensuring meaningful private sector participation. Additionally, the commission should have an appropriate mandate and the resources to engage academia to conduct relevant research that informs the commission’s deliberations.

Governments may also designate an intergovernmental task force/group to develop CNI/CII identification governance and process recommendations. Such a group should fully represent governmental stakeholders and ideally be co-chaired by representatives of the government’s technical, economic, and national security institutions which should have equal voice in developing CNI/CII identification processes. If a government designates a single agency to develop CNI/CII identification recommendations, it should take steps to ensure that the concerns/mission of that agency does not hinder or overly influence multi-stakeholder participation in the development of CNI/CII recommendations.

Factors to Consider while Preparing for Conducting CNI/CII Risk Assessments

As indicated, identifying CNI/CII is fundamentally a matter of classifying the risk exposure that information and communications technologies introduce to assets and functions that are important to national goals, objectives, and aspirations. The key to determining risk is designing an effective formal, inclusive, and rigorous governance structure and process to enumerate, define, and validate important cyber risk exposures, in particular developing a consensus on the potential harms of critical infrastructure disruptions to security, the economy, and citizens.

Most conventional approaches for dealing with cyber risks are focused on cyber-threats, attack types and vectors rather than on impact (e.g., economic, national security, societal) caused by cyber means. To date, attempts to identify and measure the harm caused by inadequate cybersecurity of critical infrastructures have used various means to express the severity of the attack. However, a threat-based approach too often encompasses a linear, cause-and-effect analysis of cyber threats. Therefore, a more holistic approach to assessing the effect of cyber threats and attacks requires the inclusion of the concept of cyber harm, which describes the negative impact upon an entity, whether individual, organizational or national.

One factor a nation may consider when developing a process to assess risks is to ‘benchmark’ certain risk assessment policy and methodological approaches that other countries have used successfully. ‘Benchmarking’ should focus on nations that have similar national goals and circumstances, including economic and political development levels, and those that have made significant advances in their CNI/CII identification efforts.

Risk assessments play an important role in helping to identify the risk tolerance of critical infrastructure owners and operators, governments, as well as other stakeholders. When a disruption in critical services occurs, the risk tolerance of an entity (whether individual, organization, or government) may vary. In some instances, cyber risks may not be a significant aspect of disruptions in services delivery, while in other cases, the disruption of distribution of basic services may be less tolerated by citizens than governments, and still must be addressed by government organizations. For instance, a disruption of electronic banking that primarily affects citizens may not have an immediate impact on national security, a government's responsibility, however, prolonged disruption of access to money could result in civil disturbances that impact national security. Similarly, critical infrastructure owners and operators, such as power generation entities, often have existing emergency procedures to deal with disruptions and recover quickly. Where these procedures exist, early government involvement may not be needed or may hinder recovery.

A country's national Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) could be a key organization for coordinating, consolidating, and analyzing risk assessments, as would sectoral CSIRTs/information sharing organizations in potential critical infrastructure sectors. If a nation does not have a designated national CERT, it should establish an organization with the requisite expertise and multi-stakeholder constituency to identify and validate the risk criteria, including thresholds of harm, that determines if a particular sector is of critical national importance. National technical standards bodies would play an important part in establishing CNI/CII classification criteria and may be excellent coordinating bodies for a CNI/CII classification effort.

Factors to Consider for Gaining Public-Private Partner Agreement on CNI/CII Classification Criteria

It is often a challenge to ensure that critical infrastructure owners and operators have a strong voice in considering the risk criteria used to designate CNI/CII. While in many countries, potential CNI/CII assets are operated by the private sector, many CNI/CII may fear greater regulation and liability risks (not to mention criminal proceedings) if their sectors or assets are deemed critical by the government. This is particularly true of industry sectors that have relatively recently adopted previously unregulated information and communications technologies to improve their operations. In other countries, the private sector may see their designation as CNI/CII as beneficial if they understand that this will give them extra attention by government, which is often required in terms of, e.g., information exchange, incident/crisis response, exercises/trainings etc. Although private sector participation in CNI/CII identification may be driven by either their prospects for avoiding regulatory risk or better mitigation of cyber risks, it is important to include their voices in establishing CNI/CII criteria. No one understands the risk to an asset or sector better than its owners and operators. Also, participation in establishing CNI/CII criteria is far more likely to be complied with if owners and operators have a say in criteria development. Lastly, substantial owner/operator participation is more likely to preserve opportunities for innovation and economic benefit.

Policymakers should also consider the characteristics of existing relationships between the government and private sector (especially critical infrastructure owners and operators) and determine whether they are conducive to meaningful partnerships that support identifying critical infrastructure and working toward national resilience goals. As mentioned above, legal frameworks are important for shaping public-private partnerships by, for instance, determining whether the relationship between government and the private sector is driven primarily by regulatory compliance or voluntary cooperation. Legal frameworks also reflect national priorities where the business objectives of critical infrastructure owners and operators may be determined to be secondary to national security, or public safety priorities.

Other characteristics of public-private relationships should also be considered including the cultural traditions of business and industry in an economy, as well as social relationships between the private sector, government, and the rest of society. In some cases, even the psychology of business leaders is important to understand, particularly in their attitudes toward how regulation may impact business innovation or profitability.

If the existing legal frameworks, government organizational structures and private sector business objectives are determined to hinder critical infrastructure identification and potentially undermine efforts to build resilience, different national policies and practices may need to be established in a NCS or similar policy to mitigate these risks. As an example, if there is no meaningful mechanism for critical infrastructure owners and operators to voluntarily participate in identifying national critical infrastructure, public policy can create such a mechanism. This type of collaborative approach may also address some of the cultural, social, and psychological aspects of public-private partnerships by helping to develop a common perspective on the importance of increasing national resilience in the face of increasing critical infrastructure threats.

Summary of Key Considerations

The most important principles for effectively formalizing CNI/CII identification include:

- A strong mandate from national leadership;

- Technical and policy competence and clear and transparent policy development processes;

- Leveraging existing laws and organizations and public-private relationships to facilitate critical infrastructure identification;

- Developing consensus on CNI/CII identification criteria and policies that are created by active participation of all partners in whatever mechanisms nations use;

- Considerations of the degree of national harm created by elements of risk – threat, vulnerability, likelihood, and predictability as well as the potential cascading consequences of prolonged disruptions.

Measures of success for formalizing CNI/CII identification process may include evidence of the government's abilities to sustain critical infrastructure identification through a comprehensive risk management process and to build a strong public-private ecosystem that facilitates the nation's ability to adapt to changing technologies and circumstances.

Section IV – CNI/CII Protection Research Needs

Public-private Partnerships on CIIP

On a strategic level, public-private partnerships (PPPs) are seen as a win-win, but there is a need to acknowledge that the goals of the parties involved are different. A model that acknowledges the structural differences in objectives from the start may be more effective.

While PPPs have become the bedrock of NCS, their operating models and incentive structure remain understudied. Acknowledging there are many benefits derived from joint action by government and industry, the diversity of forms that PPPs can take often hides an important set of challenges that are underestimated when CNI/CII protection is discussed. As attacks against CNI/CII continue to multiply and expose vital vulnerabilities, more attention needs to be paid to the type of partnerships set in place and to unpacking the differences in objectives, in particular in relation to beneficiaries. A large amount of critical infrastructure is owned and managed by the industry, yet there is little discussion about the strengths, weaknesses, and outcomes on which a PPP can build to be more effective and better secure CNI/CII. Such an understanding of capabilities and limitations in both the private and the public sector can help optimize the solutions available and clarify the goals and incentives for each of the entities involved, in order to build a stronger foundation for collaboration.

Societal Impact and Resilience

The CNI/CII identification process in the NCS context needs to focus on more than national security domains and key economic sectors. Expanding the scope of what needs to be protected to essential services whose disruption would be consequential for a country can help increase societal resilience. When designing national CNI/CII protection strategies, national security considerations generally determine the selection of sectors considered of vital importance in a specific jurisdiction. The societal impact and resilience of essential sectors often comes second, although disruptions to sectors such as healthcare, food and education can be equally consequential. As the COVID-19 pandemic has shown, the designation of critical services needs to reflect societal consequences and be based on a clear identification of the national priorities in both peaceful and crisis situations. The whole-of-society impact and resilience approach thus needs to be an integral part of the consultations of preparing related national policies, plans and strategies.

Transnational Dimensions of CNI/CII protection

Discussing risks only in relation to the national level may be limiting the protections available, as the threat outlook is increasingly global.

The dominant approach in CNI/CII protection has been based on risks at the national level, yet the threat landscape is constantly evolving. The large majority of cyber threats has important transnational dimensions that are often not accounted for in the design of national strategies. To better secure CNI/CII, additional protections should be considered at the international level via transnational instruments and collaboration. Transnational engagements can thus complement the range of actions available to relevant stakeholder in a given jurisdiction and help coordination across borders to expand the spectrum of collaboration in direct response to international threats. What is currently missing is the identification of commonly accepted criteria for CNI/CII that have global reach and impact beyond a national context and the introduction of international protections.

National cybersecurity strategies do often include Key Performance Indicators (KPIs) for CIIP, such as existence of a method for the identification of CNI/CII or involvement of relevant private, public and civil stakeholders. However, these KPIs are often too general and are not tailored to reflect specific requirements and needs. In order to allow policymakers to better track the success of the implementation of strategic objectives in CNI/CII protection area, the process of setting of actionable KPIs should be based on detailed risk assessment approach which identifies and prioritizes implementation of programs and policies designed to protect CNI/CII.

Operational Technologies

Current critical infrastructure related strategies and legislations are often IT oriented and do not take into account practices and requirements tailored for Operational Technologies (OT)/Industrial Control Systems (ICS).

Cybersecurity strategies developed for data-centric information technology are not necessarily the best fit for protecting operational technology.

As we live in the era of continuously growing IT and OT convergence, we need to find a more coherent and balanced approach to understand what each environment does and how they differ from each other. This new approach should inform and lead security decisions on strategic, operational and technical levels.

Conclusion and Outlook

This white paper draws attention to a gap that was identified in the *"Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle"* (GFCE, 2021). Advice on risk assessments methods for CNI/CII though CNI/CII protection is a foundational task for any country to protect its institutions, citizen and services, and is a key topic on the agenda of the international cybersecurity capacity-building community. There is no standard methodology to help nations formally identify and define CNI/CII in the first place in a systematic, contextualized way that informs CNI/CII protection and risk mitigation governance structures.

The white paper explores how to fill this gap by outlining three foundational elements related to CNI/CII identification in the context of NCS development and aims to encourage cybersecurity capacity-building actors to create a globally applicable and locally adoptable methodology that helps countries to develop and implement processes for CNI/CII identification as part of their NCS cycle.

Additionally, the paper highlights areas for research related to CNI/CII protection. Due to the fast development of ICTs, they are today an integrated part of critical infrastructures, facing an evolving threat landscape. Existing approaches to CNI/CII protection may not be sufficient for these changing requirements and there is to adapt or to develop new approaches.

Sources

Council of Europe (2021): Convention on Cybercrime, https://www.coe.int/en/web/cybercrime/the-budapest-convention

CyberPeace Institute (2021): Playing with Lives: Cyberattacks on Healthcare are Attacks on People. Strategic Analysis Report. Geneva: CyberPeace Institute, https://cyberpeaceinstitute.org/publications/sar001-healthcare/Global Forum on Cyber Expertise (2021)

Catalog of Project Options for the National Cybersecurity Strategy (NCS) Cycle, https://cybilportal.org/tools/catalog-of-project-options-for-the-national-cybersecurity-strategy-ncs-cycle/

United Nations (2021). Report of the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of international security, (A/76/135) https://www.un.org/disarmament/group-of-governmental-experts/