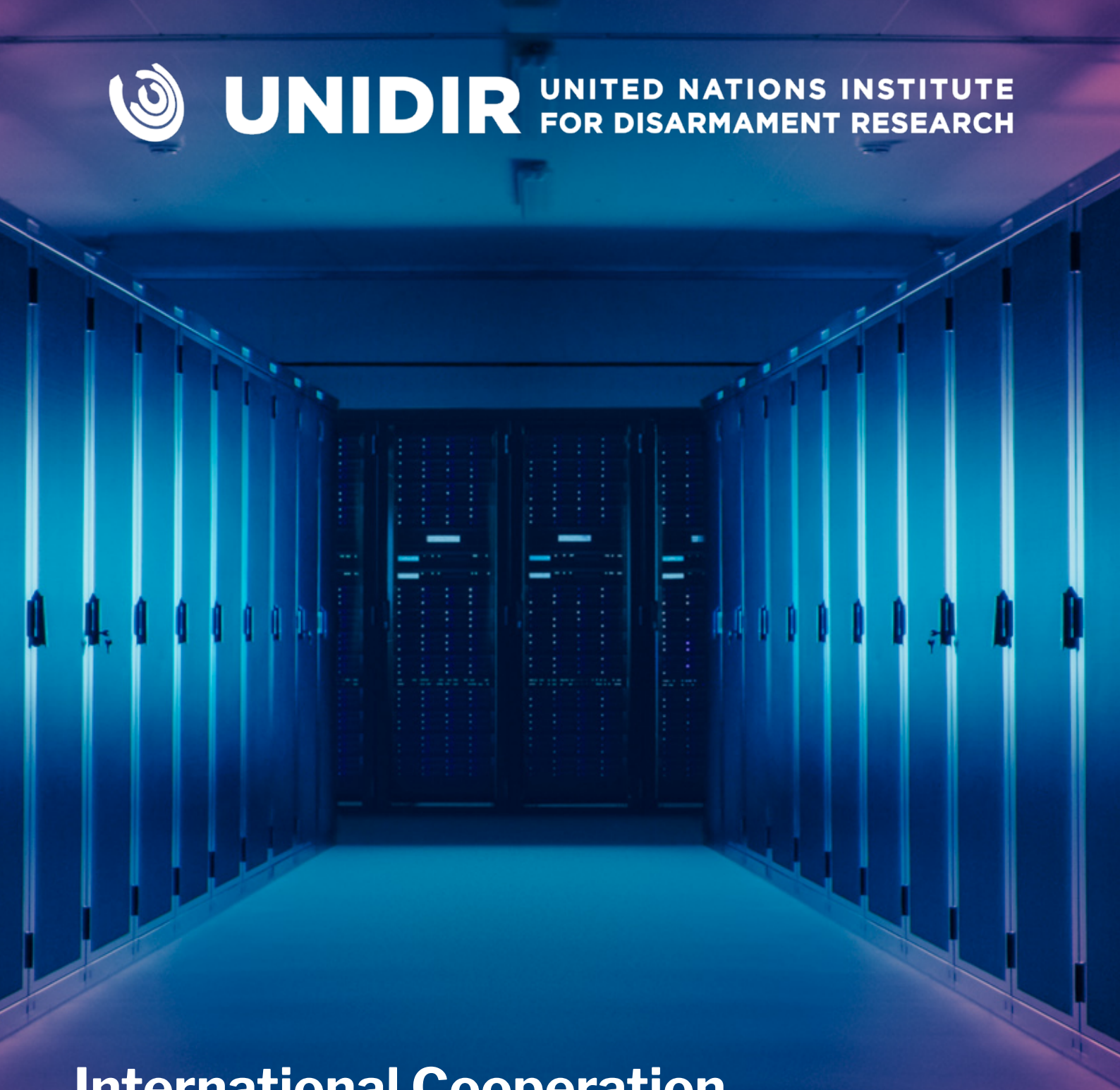
UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH



International Cooperation to Mitigate Cyber Operations against Critical Infrastructure

Normative Expectations and Emerging Good Practices

ANDRAZ KASTELIC

ACKNOWLEDGEMENTS

Support from UNIDIR's core funders provides the foundation for all the Institute's activities. This study was produced by the Security and Technology Programme's Cyber Stability workstream, which is funded by the Governments of France, Germany, the Netherlands, Norway and Switzerland, and by Microsoft. The author wishes to thank the following individuals for their invaluable advice and assistance on this report: Kerry-Ann Barrett (Organization of American States); Giacomo Persi Paoli (UNIDIR); and the participants of our multi-stakeholder dialogue, "Operationalizing Cyber Norms: Critical Infrastructure Protection," held on 3 July 2020: Oleg Abdurashitov (Kaspersky), Kaja Ciglic (Microsoft), Marc Henauer (National Centre for Cyber Security, Switzerland), Wolfram von Heynitz (Federal Foreign Office, Germany), Daniel Klingele (Federal Department of Foreign Affairs, Switzerland), Timo S. Koster (Ministry of Foreign Affairs, the Netherlands), Chris Kubecka (HypaSec) and Andre Salgado (CITI Group). Gratitude is extended also to Evgeny Goncharov, Gleb Gritsai and Anastasiya Kazakova of Kaspersky for their insight into the industry.

Design and layout of the publication: Eric M. Schulz

Graphs: Uros Podgorelec

NOTE

TABLE OF CONTENTS

ABOUT THE AUTHOR

ANDRAZ KASTELIC is the lead Cyber Stability Researcher of the Security and Technology Programme at UNIDIR. Prior to joining UNIDIR, he held various research positions at international organizations and research institutions around the world.

ABOUT UNIDIR

The United Nations Institute for Disarmament Research (UNIDIR) is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

ABBREVIATIONS & ACRONYMS

GGE	GROUP OF GOVERNMENTAL EXPERTS
ICT	INFORMATION AND COMMUNICATIONS TECHNOLOGY
OEWG	OPEN ENDED WORKING GROUP
UN	UNITED NATIONS
UNIDIR	UNITED NATIONS INSTITUTE FOR DISARMAMENT RESESARCH

EXECUTIVE SUMMARY

Malicious cyber operations pose a threat to critical infrastructure and thus to the well-being of our societies. Major incidents have the potential to both destabilize States and endanger international peace and security.

To address the risk of increasingly complex and effective cyber threats aimed at critical infrastructure, the international community uses norms of expected behaviour of States in cyberspace to promote cooperation. This report investigates the norm – as proposed in 2015 by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – that urges States to respond to international requests for assistance or mitigation in the event of malicious cyber operations against critical infrastructure.[1]

The report suggests the following measures that States and the international community should take to implement this norm:

- States should develop a clear definition of their national and international critical infrastructure, identify sectors whose products or services qualify as critical infrastructure and maintain a list of critical assets. These definitions and designations should be shared with the international community as a confidence-building measure.
- States should establish crisis resolution networks among relevant domestic actors.
- The international community should establish a network of single points of contact within the competent national entities and authorize these points of contact to communicate with their international counterparts.
- States should regularly test their capacity to communicate with other States, as well as their capacity to respond to requests for assistance and mitigation (particularly channels of communication, protocols and procedures), by way of international cybersecurity exercises.

1 UNGA (2015b, III: para. 13(h)).

- When communicating requests for assistance or mitigation, States do not need to seek the establishment of universal international protocols but should follow existing best practices pertaining to incident reporting in the relevant international and national contexts.
- All States that may engage in cooperative efforts to respond to malicious cyber operations against critical infrastructure should use pre-established domestic multi-stakeholder crisis resolution networks and lean on the mitigation expertise provided by the State as well as non-State actors in the event of a cyber operation of this type.
- Note that normative expectations of assistance and mitigation are dependent on the context. In the event of a malicious cyber operation against critical infrastructure, the State from which the operation is launched (in other words, the State of emanation) should take reasonable measures to either terminate the cyber operation in question or minimize the propagation of malicious code central to the cyber operation itself.
- Any State that receives a request to assist should do its utmost to provide help in the form requested by the State affected. The concept of assistance is not limited to direct action against the malicious cyber operation but can entail any form of help that minimizes the consequences of the cyber operation against critical infrastructure.

1. Understanding the context and the problem

Malicious cyber operations against critical infrastructure – that is, all assets essential for the maintenance of functions vital to the well-being of a given society[2] – pose a threat not only to the well-being of the targeted State but also to international peace and security.[3] Sectors that typically fall within definitions of critical infrastructure include energy, transport, health care, government, food production and supply, water supply, financial services, telecommunications, and critical manufacturing.[4]

Although the specific extent and effects of cyber incidents affecting critical infrastructure cannot be reliably established, recorded instances testify to the devastating potential of such incidents. Due to the essential nature of critical infrastructure, cyber incidents that impact it can have dire consequences for our societies, including economic ramifications, material damage and even injury to human beings.

In 2015, the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE) proposed an international norm aimed at facilitating international cooperation in the event of a cyber operation against critical infrastructure. This report is intended to aid understanding of how to operationalize said norm; the report is structured as follows:

- The remainder of the first section details the challenges associated with protecting critical infrastructure from cyber threats and outlines the aforementioned norm.
- The second section enumerates preparatory steps that individual States should consider implementing before a cyber incident occurs.
- The third section recommends actions to be implemented at the international level.
- The fourth section proposes measures for implementing the GGE norm after the occurrence of a cyber incident.
- The fifth section notes some unresolved questions and suggests directions for future international discussion or research.

1.1 PREVALENCE OF CYBER INCIDENTS AFFECTING CRITICAL INFRASTRUCTURE

Recently, several notorious cyber operations have crippled various critical infrastructure.[5] However, it remains challenging to ascertain the exact number of such incidents and, therefore, whether they are becoming more common or disruptive. This challenge results from:

2 There is no internationally agreed definition of critical infrastructure. This report adopts a working definition inspired by the Council of the European Union (2008, art 2(a)), although some alternative examples are given (see section 2.1).
3 OEWG (2021, para. 18).
4 Which sectors are considered critical depends on the context. See section 2.2.
5 See, for example, Steffen (2016) on a string of cyber operations against German hospitals; Gallagher (2020) on cyber operations against health care institutions around the world; the US Cybersecurity and Infrastructure Security Agency (2020) on cyber operations causing loss of productivity and revenue at a natural gas compression facility; and Statt (2021) on a cyber operation interfering with a water treatment plant.

- Definitional variations among countries and sectors
- Different approaches to measuring the frequency and impact of cyber operations
- High uncertainty on the actual number of cyber operations

The first reason for this challenge of quantification is that the concept of critical infrastructure is not clearly or universally defined; its meaning depends significantly on the national context. For example, while some States rely on the tourism sector for a sizeable portion of their gross domestic product and might therefore qualify the underpinning infrastructure as critical,[6] the same sector may not be as crucial for other States. Thus, any statistics indicating trends of cyber incidents against generally defined "critical infrastructure" should be read with caution.

What is more, critical infrastructure is a multifaceted concept, and different sectors exhibit different cyber incident trends. It would be a generalization to say that malicious cyber operations targeting every sector of critical infrastructure are on the rise or in decline: a more granular, sector-specific analysis is required to fully assess the evolution of the threat landscape.

Lastly, many of the malicious cyber operations affecting critical infrastructure can go either undetected or unreported. As such, the number of recorded cyber incidents affecting critical infrastructure could be higher than available statistics and reporting would indicate. Kaspersky reports that the majority of cyber incidents affecting critical infrastructure remain undisclosed and unknown to the public, be it a result of explicit requests from the infrastructure operators or because infrastructure operators are precluded from disclosing such incidents by local legislation.[7] Similarly, the International Committee of the Red Cross emphasizes "the difficulty of assessing how many operations remained undetected, how much reach the attackers really had into the infrastructure, or whether backdoors had been established for future use, for example as kill switches".[8]

It is thus perhaps unsurprising that that research by different security companies reflect differing, at times contradictory, trends. For instance:

- IBM reports that the number of cyber incidents affecting industrial control systems and operational technology networks – frequently used by critical infrastructure – was higher in 2019 than in the previous three years combined.[9]
- Research done by Kaspersky indicates that the proportion of industrial control system computers targeted by malicious code has actually been in decline in the second half of 2019 and the first half of 2020. The trend has reversed only in the second half of 2020.[10]

6 See, for example, Republic of Mauritius (2014).
7 Personal correspondence with Evgeny Goncharov, Head, Kaspersky Lab ICS CERT, October 2020.
8 Gisel & Olejnik (2019, 25).
9 IBM X-Force Incident Response and Intelligence Services (2020, 6).
10 Kaspersky ICS CERT (2020b, 13, 15); Kaspersky ICS CERT (2021).

1.2 CONSEQUENCES OF A DISRUPTION OF CRITICAL INFRASTRUCTURE

Regardless of the exact number of cyber operations against critical infrastructure, enough real incidents have occurred to justify broad concern over maintaining the security of increasingly connected critical infrastructure. In early 2020, for example, a malicious cyber operation aimed at the Brno University Hospital in Czechia forced the facility to suspend its scheduled surgeries and divert patients to nearby facilities.[11] Four years prior, Ukraine's electricity distribution company reported a network outage of several hours' duration due to a cyber operation targeting their computers and supervisory control and data acquisition systems. Approximately 225,000 customers experienced power shortages.[12]

Not all cyber operations against critical infrastructure cause outages of critical services, although they do offer an insight into possible grave consequences. For instance, in April 2020, Israel's authorities reported a cyber operation against the country's water treatment systems, attempting to spoil the regional waterways.[13] A similar incident was recorded in early 2021 at a water treatment facility in Florida.[14]

Over the last decade, an increasing number of national governments have joined private enterprises[15] and security professionals[16] in recognizing these types of incident among the most prominent cybersecurity issues. In 2015, the GGE noted in its report that "the risk of harmful [information and communications technology] attacks against critical infrastructure is both real and serious".[17]

By definition, the disruption of critical infrastructure could have wide-reaching consequences and dangerously undermine vital functions that societies rely on, as well as potentially result in physical destruction and human injury or death.[18] For example, a well-executed cyber operation against key energy distribution elements could, at least in theory, deprive an entire country of electricity.[19] Although the exact consequences of the aforementioned cyber operation against the Ukrainian electricity supply system remain unknown, the economic ramifications following other past local[20] and nationwide[21] power outages have been well documented. Power outages have also been proven to result in an increase of the levels of non-accidental mortality.[22]

Cyber operations targeting other infrastructure may not directly result in injury to human beings but can severely cripple a society. For instance, if used to target national and international financial systems, malicious use of information and communications technology (ICT) could "endanger financial stability"[23] and thus all the aspects of a functioning society relying on stable finan-

---

11 Khalili (2020).
12 Lee et al. (2016).
13 Cimpanu (2020).
14 Statt (2021).
15 Siemens Gas & Power (2019).
16 ENISA (2019, 109); Security Magazine (2020)
17 UNGA (2015b, II: para. 4).
18 During the 2020 Open-ended Working Group on developments in the field of information and telecommunications in the context of international security meeting, States emphasized that attacks on critical infrastructure "pose a threat not only to security, but also to economic development and livelihoods, and ultimately the safety and wellbeing of individuals" (OEWG, 2020, para. 22).
19 Smith et al. (2019).
20 Shuaia et al. (2018).
21 Schmidthaler & Reichl (2016).
22 Anderson & Bell (2012).
23 G-20 (2017, para. 7).

cial flows. The 2007 cyber operation against, inter alia, the banking sector of Estonia prevented the population from using online banking. Even though the Estonian computer network infrastructure sustained no physical damage, the country, where 97% of bank transactions occur online,[24] was said to be temporarily crippled.[25]

1.3 CHALLENGES OF MANAGING CYBER THREATS AGAINST CRITICAL INFRASTRUCTURE

The risk of dire consequences following a critical infrastructure incident is exacerbated by the evolving cyber threat landscape, which is characterized by a range of factors:

- New and increasingly complex attacks.[26] Malicious actors are continuously devising new attack vectors and developing corresponding exploitations. Nowadays, malicious software targeting critical infrastructure is becoming more and more tailored to the target and thus more sophisticated.
- Rapid expansion of the attack surface.[27] This is mostly due to the growing interconnectedness of ICT systems employed in critical infrastructure assets. Teleworking arrangements implemented as a response to the COVID-19 pandemic have accelerated or compounded this problem.[28]
- Outdated legacy systems that are not sufficiently resilient to new threats and contribute to the expanding vulnerability of critical infrastructure. For example, according to a US congressional report, industrial control computer systems, an integral part of critical infrastructure, are "specific points of vulnerability, as cyber-security for these systems has not been previously perceived as a high priority."[29] Similar assessments have been advanced by, for example, Microsoft[30] and scholarship contributions.[31]
- Insufficient resources allocated to prevention efforts.[32] For instance, the 2018 cyber operation that severely affected the ability of the UK National Health Service to provide

24 Herzog (2011, 51).
25 Ilves (2007).
26 "The threat landscape is becoming extremely difficult to map. Not only attackers are developing new techniques to evade security systems, but threats are growing in complexity and precision in targeted attacks" (ENISA, 2020c). And as Kaspersky notes, "threats are becoming more targeted and more focused, and as a result, more varied and complex" (Kaspersky ICS CERT, 2020b).
27 For example, according to Bhunia & Tehranipoor (2019, ch. 1), "Attack surface is the sum of all possible security risk exposures". In other words, attack surface represents the set of potential access points that malicious actors can exploit in the course of the perpetration of a cyber operation. See also the predictions by ENISA (2020c, 10).
28 See, for example, US CISA (2020b)
29 Shea (2004).
30 "Operational technology (OT) networks used in industrial and critical infrastructure environments have traditionally been air-gapped from corporate IT networks and the internet, but digital transformation has increased both the connectivity and number of devices in these environments, leading to higher risk. Further increasing risk, many of the legacy IoT [Internet of Things]/OT protocols and embedded devices in these environments were designed years ago—lacking modern controls such as encryption, strong authentication, and hardened software stacks" (Microsoft, 2020, 31).
31 For example, "healthcare organizations and universities often lack resources to protect against cyber-attacks", as argued by Muthuppalaniappan & Stevenson (2020).
32 BBC (2017); Maglaras et al. (2018, 42).

care[33] might have been prevented had the operators dedicated resources and patched (and thus immunized) the computer systems prior to the incident.[34] Lack of diligence is certainly not unique to this example; it can also be observed in other jurisdictions and critical infrastructure sectors.[35] According to Microsoft, 71% of industrial control systems rely on outdated versions of the Windows operating system that are no longer regularly updated with security patches by Microsoft.[36]

- Unpredictability of effects, including their reach. The interdependencies between critical infrastructure is a well-documented phenomenon, and cyber incidents can have unpredictable and wide-reaching negative consequences, stretching well beyond the territorial borders of one country. The effect of such interdependencies can be seen in the November 2006 failure of the electric grid element in Germany, which resulted in power shortages in 20 countries in Europe and beyond, impacting around 15 million households.[37] Although this incident was not a result of a cyber operation, it is illustrative of the potential widespread disruption cyber operations against critical infrastructure could cause.

33 Ghafur et al. (2019).
34 Morse (2017).
35 See, for example, US DOE (2019).
36 Microsoft (2020, 31).
37 Van der Vleuten & Lagendijk (2010).

1.4 PROTECTING CRITICAL INFRASTRUCTURE: THE INTRODUCTION OF NORMS

All the factors described in the preceding section point to the need for international collaboration to prevent or mitigate malicious cyber operations aimed at critical infrastructure. One approach the international community has been pursuing in the past decade to secure critical infrastructure, elevate (inter)national security and prevent possible devastation and harm to human beings is centred on norms of responsible behaviour in cyberspace.[38]

To "reduce risks to international peace, security and stability"[39] and, in particular, to minimize the impact of malicious cyber operations against critical infrastructure, the 2015 GGE proposed three specific norms of responsible State behaviour in cyberspace, elaborating the expectations of the behaviour of States in relation to the security of critical infrastructure in the cyber era. These norms indicate that States should:

- Refrain from conducting cyber operations against critical infrastructure under a foreign jurisdiction
- Protect their own critical infrastructure from malicious cyber operations
- Consider international cooperation in the event of a malicious cyber operation against critical infrastructure [40]

OTHER NORMS OF RESPONSIBLE STATE BEHAVIOUR IN THE CONTEXT OF CRITICAL INFRASTRUCTURE

The fact that the international community puts critical infrastructure protection at the top of the list of international cybersecurity concerns is evident also from the emergence of similar or related norms envisioned and promoted by various consortiums. For instance, members of the Paris Call for Trust and Security in Cyberspace pledged to work together, in the existing forums and through the relevant organizations, institutions, mechanisms and processes, to assist one another and implement cooperative measures, notably to prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.[41] These norms would help bridge the digital divide, exemplify good neighbourliness, increase the effectiveness of incident responses[42] and generally contribute to the stability and security of the interconnected world. This is especially so if the critical element of the infrastructure stretches beyond the borders of one nation, as is the case with international or supranational critical infrastructure,[43] such as the public core of the Internet.[44]

38 Technological solutions, international law, capacity-building and confidence-building measures, and so on, also play an important role, although the exploration of these is beyond the scope of this report. See, for example, Baker et al. (2020, 503); Gusev (2020, 314); UNGA (2015b, V).
39 UNGA (2015b, para. 10).
40 UNGA (2015b, para. 12(f)–(h)).
41 Ministry of Europe and Foreign Affairs, France (2018).
42 NIST (2012, 45).
43 OEWG (2020, 17).
44 Government of the Netherlands (2017; 2020, 2).

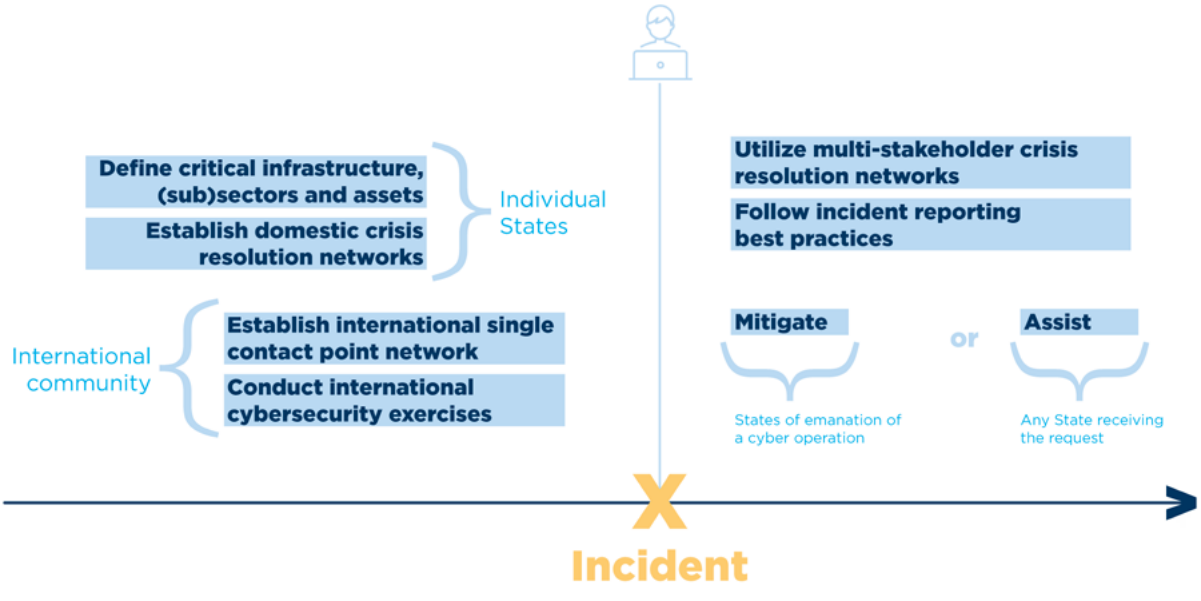
1.5 DEFINING THE SCOPE OF THIS REPORT

While the three norms included in the 2015 GGE report, and described above, are interconnected and mutually reinforcing, **this report focuses on the issue of international assistance** and more specifically on how States can be better prepared to request or respond to such assistance when necessary.

Although a wealth of research on critical infrastructure protection exists,[45] the international assistance and mitigation requirements in the context of critical infrastructure protection have not been recorded, especially not in the context of the relevant GGE norm. While the focus of this norm is on the response to malicious ICT acts against critical infrastructure, its implementation relies on a series of actions and activities at the national, regional and international levels undertaken before and after the incident takes place. Such activities, which are discussed in detail throughout the report, are summarized in Figure 1.

Many of the actions and activities discussed in this report are relevant to achieving an enhanced national capacity to prevent, mitigate and respond to or recover from malicious cyber acts against critical infrastructure. However, the focus of the report remains on the modalities of international cooperation, and as such the measures described do not cover the whole range of factors to consider in the broader context of cyber capacity development. In particular, the report does not discuss the preventive measures States could put in place in order to avoid the cyber incident from materializing in the first place.

FIGURE 1:
Actions suggested by this report to ensure operationalization of the analysed GGE norm



45 See, for example, ENISA (2020a).

2. Implementing the norm: national preparatory actions

Operationalization of the GGE norm requires the development of enabling national structural frameworks in advance of any potential malicious cyber event to ensure a sufficient level of preparedness. As such, **States should adopt a general definition of critical national infrastructure, identify qualifying (sub)sectors and compile a list of relevant assets; they should also establish domestic crisis resolution networks.**

States seeking guidance on the process of defining critical national infrastructure, sectors and assets can make use of various assistance programmes,[46] guiding documentation[47] and collections of existing national good practices[48] compiled by international organizations.

2.1 WHICH INFRASTRUCTURE IS IN FACT CRITICAL?

It is every State's sovereign prerogative to determine the scope of critical infrastructure. Not only does this align with the principle of sovereignty in international law but it has also been explicitly confirmed by United Nations Security Council resolution 2341, affirming that "each State determines what constitutes its critical infrastructure".[49]

That said, infrastructure may be classified as critical on the basis of its purpose, on the basis of the effects of a disruption to the assets or services that the infrastructure enables, or on the basis of a hybrid of the two principles.[50] Several regional attempts to specify the scope of critical infrastructure have been proposed and may provide guidance to States. For instance, the Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization defines critical infrastructure as encompassing "facilities, systems and institutions of the state, the impact on which may have consequences directly affecting national security, including the security of an individual, society and the state".[51] Similar general definitions of the concept are provided by other international and regional frameworks, such as the Organization of American States' Declaration on Protection of Critical Infrastructure from Emerging Threats[52] and the African Union Convention on Cyber Security and Personal Data Protection.[53]

46 See, for example, CICTE (2015, para. 9)
47 OECD (2008b); Suter (2007).
48 UNCTED & UNOCT (2018).
49 UNSC (2017, 2). The national prerogative has been adopted by certain regional frameworks, such as African Union (2014, art. 24). See also, for example, ITU (2010).
50 UNCTED & UNOCT (2018, 58).
51 Shanghai Cooperation Organization (2009, 10).
52 CICTE (2015, para. 11).
53 African Union (2014, art. 1).

2.2 DESIGNATING RELEVANT SECTORS AND SUBSECTORS

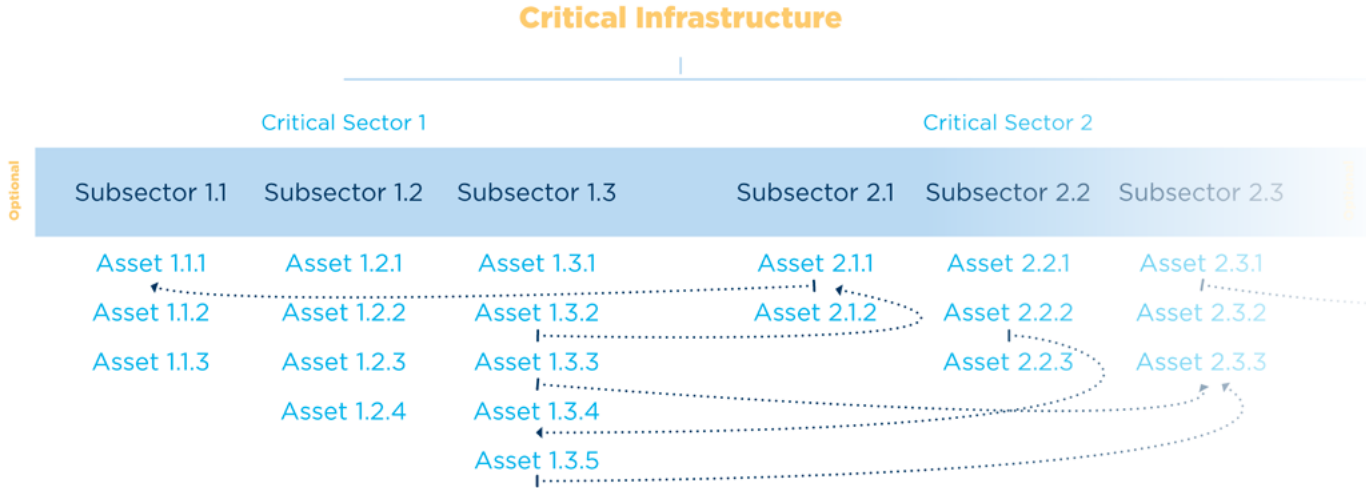
Following the adoption of a definition, **States should designate qualifying sectors (and possibly, subsectors) that are to be considered critical national infrastructure.** While the definitions of critical infrastructure will probably exhibit a degree of coherence among nations, the lists of sectors designated as critical will undoubtedly be different.

Sectors considered critical are often those whose disruption would likely lead to human harm, widespread material damage, and economic and social instability. In this context, sectors such as energy, finance, water and food supply, transportation, ICT, and government are likely to be considered critical by most States.[54] However, sectors such as tourism may be identified as critical only by a selection of States whose economies heavily rely on those sectors.[55]

2.3 COMPILING AND MAINTAINING A LIST OF CRITICAL ASSETS

States should compile and maintain a list of national critical assets. This list should include specific entities or assets that enable the functioning of the previously determined critical (sub) sectors. Taking into account the sensitive nature of such a list due to its potential national security implications, States should ensure proper communication and information-sharing with relevant parties, including the asset owners or managers. The list should also be organized into different priority groups based on the vulnerability of the assets and the gravity of the impact the malfunctioning of one would have. The list can also include assets qualifying as international critical infrastructure, located outside the jurisdiction of a particular State yet considered to be critical to the functioning of its society. It is imperative that States regularly review their lists of critical assets, along with priority group allocations, to remain abreast of changing national circumstances as well as the evolving cyber threat landscape.[56]

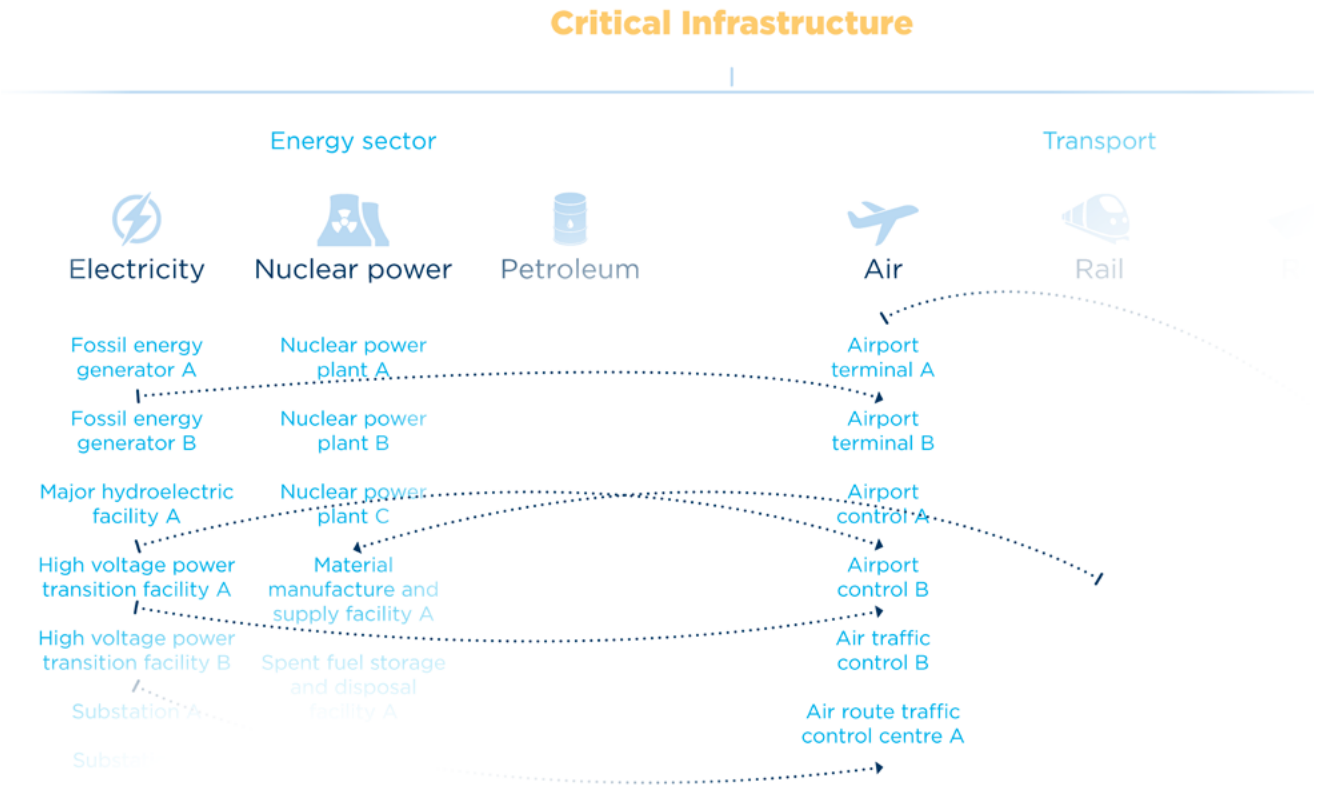
FIGURE 2:
Theoretical structure of national critical infrastructure (sectors, subsectors, assets), showing interdependencies



54 See, for example, Federal Office for Civil Protection, Switzerland (2020).
55 See, for example, Republic of Mauritius (2014, 11).
56 Global Cyber Security Capacity Centre (2016).

There may be interdependencies among certain assets. If, for instance, a cyber operation disables a specific high-voltage power transition facility, it is likely that assets belonging to a different sector will be severely affected, perhaps even disabled, in the absence of appropriate redundancies.

FIGURE 3:
Example structure of national critical infrastructure, showing sectors, assets and interdependencies



Inherent progress, consequential deflation of the prices of technology and the rapid digitalization processes accelerated by the COVID-19 pandemic are driving the increase in the number of assets considered critical, therefore expanding the scope of critical infrastructure. However, States should avoid the temptation of stretching the concept of critical national infrastructure beyond its limits: the more extensive the defined scope of critical infrastructure, the more extensive the strategic investment generally required by the government, as well as by critical infrastructure operators, to protect that infrastructure.[57] For this reason, States should consider limiting the concept of critical infrastructure to the assets and sectors that are truly *vital* to the well-being of society.

57 This report does not address the operationalization of the norm suggesting that States invest in protecting their critical infrastructure. Many attempts to outline the protection of critical infrastructure exist. See, for example, Federal Ministry of the Interior, Germany (2009); OECD (2008a).

2.4 ESTABLISHING DOMESTIC CRISIS RESOLUTION NETWORKS

In addition to defining the concept of critical infrastructure, States should **consider establishing multi-stakeholder crisis resolution networks among the relevant domestic actors.** These should be inclusive in nature and actively engage State entities and representatives of the private sector, inter alia, critical infrastructure operators, private computer emergency response team and other competent actors willing and able to contribute to the successful resolution of a cyber incident affecting critical infrastructure at home or abroad. Additionally, this type of networks could also contribute to prevention efforts.

Aside from the established communications channels, documented lean domestic protocols and procedures allowing for a swift flow of information from the critical infrastructure operator or national competent authority (for example, a computer emergency response team) to a national point of contact are necessary for the effective issuance of a request for international assistance or mitigation. Much like the collaborative entities in the international arena, domestic stakeholders should be familiar with the agreed protocols and processes.[58]

58 Similar suggestions are made in UNCTED & UNOCT (2018, 58).

3. Implementation through international community engagement

In addition to the internal efforts to establish domestic crisis resolution networks, the efficiency, effectiveness and timeliness of international cooperation in response to a malicious ICT act against critical infrastructure would benefit from the following actions at a regional and international level:

- Increased transparency and information-sharing on the subject of critical infrastructure, including on definitions and scope
- Establishment of dedicated channels for communication among clearly identified points of contact
- Development of protocols and procedures to support information flows across national and international communication channels
- Regular regional and international exercises to test the correct functioning of the networks of points of contact, protocols and procedures

3.1 TRANSPARENCY AND INFORMATION-SHARING

States should practice transparency and foster regular exchange of information pertaining to the national conceptualizations of critical infrastructure. To that end, the 2015 GGE urged States to subscribe to the "voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure".[59] Information-sharing is one of the key enablers for international cooperation, assistance and mitigation in the context of critical infrastructure being disrupted by a malicious cyber operation. It not only supports States in better communicating their needs in times of crisis but also enables a better assessment of the required response by States receiving requests for assistance (or mitigation).

Various regional and international repositories exist to facilitate this exchange of information. One such project is UNIDIR's Cyber Policy Portal,[60] a digital repository of the national cybersecurity policy landscape across United Nations Member States, regional intergovernmental organizations and multilateral frameworks. Another example is the National Cybersecurity Strategies Repository, maintained by the International Telecommunication Union.[61]

59 UNGA (2015b, para. IV(d)).
60 www.cyberpolicyportal.org
61 ITU (2020).

3.2 SINGLE POINTS OF CONTACT

Established and institutionalized communication channels among the relevant members of the international community will help ensure the effective and swift flow of information in the event of a disruption of a member's critical infrastructure. **The international community should aim to establish a global network of single points of contact within the competent national entities, authorized to communicate with their international counterparts** when the situation calls for it.[62] An example of such a network is the list of single points of contact established by the European Union NIS Directive,[63] which is regularly updated and freely available online.[64]

The 2015 GGE report recommended that States consider establishing the directory of points of contact "at the policy and technical levels."[65] During the debate of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) in February 2020, several delegations[66] spoke in favour of establishing a global list of points of contact but did not take a unified position on the nature or competence of the entities in this directory. Some delegations argued in favour of political points of contact; others preferred a list with multiple points of contact representing computer emergency response entities, law enforcement and other relevant stakeholders.[67] The final OEWG substantive report included a recommendation that States establish a global directory of points of contact.[68]

Assistance and mitigation can take a multitude of other, non-technical forms.[69] However, to reduce the risk of confusion and uncertainty at times of crisis, it is suggested that any future list of points of contact include only the officially endorsed national entities with adequate technical and operational knowledge to either request or facilitate international assistance and mitigation.

---

62 Proceedings of the Multi-stakeholder Dialogue on Operationalizing Cyber Norms: Critical Infrastructure Protection, 3 July 2020 [on file with the author]. The idea has also been advanced by the 2015 GGE report: see UNGA (2015b, IV (a)).
63 EU (2016, art. 8).
64 EC (2020). See also G-7 (2019); OSCE Permanent Council (2013, art. 8). Although in a slightly different, narrower context, the Convention on Cybercrime also requires States to designate national points of contact in order to facilitate the fight against cybercrime. See CoE (2004, art. 35).
65 UNGA (2015b, para. 16(a)).
66 Argentina, Australia, Brazil, Canada, Chile, Colombia, Ecuador, Estonia, France, Ghana, Malawi, Malaysia, Mexico, New Zealand, Russian Federation, Slovenia, Switzerland and Syrian Arab Republic (Gavrilović, 2020).
67 Gavrilović (2020).
68 OEWG (2021, para. 51).
69 See section 4.3.

3.3 CONDUCTING (INTER)NATIONAL CYBERSECURITY EXERCISES

Successful international cooperation is conditioned by functional crisis resolution networks and by effective protocols and communication channels. It is therefore suggested that States regularly **conduct national and international cybersecurity exercises** that will test their capacity to communicate, or respond to, requests for assistance and mitigation.

National cybersecurity exercises will evaluate and strengthen the preparedness of domestic crisis resolution networks and their capacity to relay appropriate requests for assistance and mitigation to other States. Additionally, such exercises will strengthen capacity to assist another State in the event of a cyber operation against critical infrastructure.[70]

International cybersecurity exercises also assist in building the capacity of States to effectively communicate a call for assistance or mitigation but particularly to strengthen the channels of communication among the points of contact, as well as the international protocols and procedures used. In addition to this, international cybersecurity exercises also facilitate confidence-building among States. The International Telecommunication Union, for example, regularly assists States in conducting regional cybersecurity exercises.[71]

70 OAS (2021) and OSCE (2018), for example, support States in conducting national cybersecurity exercises.
71 ITU (2021).


NEW YORK
SYDNEY

4. Responding to a cyber incident in the context of the norm

As it stands, the GGE norm calling for international cooperation in an effort to stop a malicious cyber operation against critical infrastructure indicates no expectations of due diligence and no requirement for the international community to proactively communicate with the State affected. According to the norm, the State whose critical infrastructure has been targeted by a cyber operation bears the responsibility of issuing an appropriate request for assistance or mitigation.

In this context, to ensure the operationalization of the norm, it has to be established what requests constitute "appropriate requests for assistance [or mitigation] by another State whose critical infrastructure is subject to malicious ICT acts".[72]

4.1 BEST PRACTICES GUIDING INTERNATIONAL COMMUNICATION

Points of contact should follow commonly recognized protocols and processes in their interaction. Given the challenges of creating universal protocols and processes for communication, **States should follow existing best practices pertaining to incident reporting in the international and national contexts.** This will allow for optimal communication between the parties involved and therefore facilitate efficient incident resolution.

The European Union Agency for Cybersecurity's *Good Practice Guide on Incident Reporting*[73] and the US Computer Emergency Readiness Team's *Federal Incident Notification Guidelines*[74] serve as examples of incident reporting frameworks that could be leveraged for this purpose. Examples of technical protocols that could be used in the same context include the Information Exchange Policy 2.0 and the Traffic Light Protocol, both published by the Forum of Incident Response and Security Teams.[75]

In addition, an appropriate request for assistance and mitigation should include not only information about the incident but also specific suggested actions to be taken by the State to which the request is addressed.

4.2 INCLUSIVE, MULTI-STAKEHOLDER APPROACH TO RESPONDING

All States engaged in the cooperative thwarting of a malicious cyber operation against critical infrastructure should **use the previously mentioned domestic multi-stakeholder crisis resolution networks and lean on the mitigation expertise provided by the State and by relevant non-State actors.** The private sector possesses a wealth of cybersecurity expertise and often controls relevant critical infrastructure technologies. As such, any attempts of crisis resolution

72 UNGA (2015b, III: para. 13 (h)).
73 ENISA (2009).
74 US-CERT (2015).
75 FIRST (2019).

without the involvement of the private sector are likely to achieve suboptimal results.[76] Once again, it is important that States invest in establishing national networks of collaboration and crisis resolution, with well-defined communication channels and clear roles and responsibilities of the network members.

4.3 THE DIFFERENCE BETWEEN ASSISTANCE AND MITIGATION

As stipulated by the norm in question, States should respond to "appropriate requests for assistance" or "appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State".[77] States that receive requests for assistance or mitigation are not expected to act beyond their means; they are simply expected to do their utmost to provide aid, with the resources available at the time. But what is the difference between assistance and mitigation?

First, when the origin of a cyber operation cannot be determined or when a cyber operation is emanating from the infrastructure of a State other than the one receiving the request, **States asked to assist are urged to provide any help or support they can to minimize the undesired consequences of the malicious cyber operation against critical infrastructure.** States can also provide assistance with terminating the cyber operation or hardening the computer network systems of the affected critical infrastructure. The aid can be supplied in various forms and is not limited to technical assistance. If a cyber operation, for instance, hinders the production of electricity in a particular State, this State can request assistance in the form of an additional supply of electricity. When assistance is requested, it is the State affected by the cyber operation that is expected to stipulate the needs or specify the request, including the extent and methods of assistance. It is important that the interacting and cooperating States communicate and act in good faith and within the boundaries of the international legal principle of sovereignty and the resulting obligations.

Second, if the request is submitted to the State from which the malicious cyber operation is believed to originate (the State of emanation), that State should respond by attempting to mitigate the cyber operation itself. Mitigation, compared with assistance, appears to be a narrower concept and refers to the act of limiting[78] the cyber operation against the critical infrastructure. As such, mitigation is largely reserved to actions of a technical nature and related to the cyber operation itself. **In this context, States of emanation are expected to take reasonable measures to either terminate or minimize the propagation of the underlying malicious code.** Although narrower in its scope than assistance, mitigation points to the important role that States of emanation have in limiting the propagation of the cyber operation and its resulting havoc. Mitigation and assistance are not mutually exclusive; a State asked to mitigate a cyber operation originating from its territory could also be providing assistance.

That being said, the norm does not account for the role of States of transit, whose infrastructure may be an important enabling link in the chain of the malicious operation and who will thus po-

76 See, for example, ITU et al. (2018, 44).
77 UNGA (2015b, para. 13(h)).
78 ICJ (1997, para. 80).

tentially also be in a position to mitigate the cyber operation against another State's critical infrastructure. The role of transit States could be further analysed by the international community as it continues to advance discussions on norms of responsible State behaviour in multilateral forums.

Third, assistance and mitigation efforts should not be centred on the issue of technical attribution. In the immediate response to a cyber operation against critical infrastructure, activities aimed at discovering the culprit should only be conducted to the extent that they limit the damage of the ongoing cyber operation. This does not mean that the actors joined in this collaborative response should neglect any digital evidence discovered during the incident resolution phase; such evidence could prove useful at a later stage and allow them to take measures in accordance with domestic criminal law or the international law of State responsibility. Nevertheless, by no means should attribution become the central effort of the cooperating parties, as it may derail them from the primary goal of the cooperation – to stop the propagation of the cyber operation and minimize its undesired consequences.

Conclusion

To minimize the impact of threats to critical infrastructure, the international community seeks to promote peace and security through voluntary norms of responsible State behaviour in cyberspace. In 2015, the United Nations General Assembly adopted a set of norms developed by the GGE, promoting, inter alia, cooperation among States in the case of a disruptive cyber operation against critical infrastructure, stating that States should respond to appropriate requests for assistance or, in certain cases, mitigation by another State whose critical infrastructure is subject to malicious ICT acts.

To facilitate and support States in the implementation of that norm, this report elaborated the scope and content of the norm, clarifying the normative expectations, State practice, and emerging good practices pertaining to the norm. Specifically, the report suggests that States:

- Define critical infrastructure, including (sub)sectors and a database of qualifying assets
- Establish domestic, multi-stakeholder crisis resolution mechanisms
- Share information on the conceptualization of critical infrastructure with the international community
- Aim to establish a global network of contact points
- Regularly conduct (inter)national cybersecurity exercises
- Follow best practices related to communication when submitting or responding to a request for assistance or mitigation
- Do their utmost to provide assistance to the affected State in whatever form requested and, if recognized as a State of emanation of a malicious cyber operation, do their utmost to mitigate the operation itself

Several aspects of the norm, however, remain to be further elaborated by the international community. Accordingly, States should continue expounding their views on the operationalization of the norm or providing additional layers of understanding by sharing good practices and experiences with implementing the norm.

Furthermore, the international community should consider exploring the role of transit States as it reflects on the implementation of the current normative framework, paying particular attention to transit States' potential to contribute to mitigation efforts in the event of a cyber operation against critical infrastructure.

The international community should also consider elaborating the concept of international or transnational critical infrastructure and define the expectations towards different States in mitigating the malicious cyber operations aimed at such infrastructure.

Lastly, the international community should consider how to leverage current and future capacity-building efforts[79] in order to strengthen the national capabilities of individual States, enabling them to protect their own infrastructure as well as to mitigate a malicious cyber operation aimed at another State's critical infrastructure or to assist the State in need.

79 UNGA (2015b, para. 23).

References

African Union. 2014. Convention on Cyber Security and Personal Data Protection. 27 June.

Anderson, Brooke G., & Michelle L. Bell. 2012. 'Lights Out: Impact of the August 2003 Power Outage on Mortality in New York, NY.' *Epidemiology* 23 (2): 189–193. As of 24 October 2020: https://journals.lww.com/epidem/Fulltext/2012/03000/Lights_Out___Impact_of_the_August_2003_Power.3.aspx

Axelrod, Robert. 1984. *The Evolution of Cooperation.* New York: Basic Books.

Baker, Thar, Muhammad Asim, Áine MacDermott, Farkhund Iqbal, Faouzi Kamoun, Babar Shah, Omar Alfandi & Mohammad Hammoudeh. 2020. 'A Secure Fog‐Based Platform for SCADA‐Based IoT Critical Infrastructure.' *Special Issue: Software Tools and Techniques for Fog and Edge Computing* 50 (5): 503. As of 21 October 2020: https://onlinelibrary.wiley.com/doi/abs/10.1002/spe.2688

BBC. 2017. 'NHS "Could Have Prevented" WannaCry Ransomware Attack.' *BBC News*, 27 October. As of 25 October 2020: https://www.bbc.com/news/technology-41753022

Bhunia, Swarup, & Mark Tehranipoor. 2019. *Hardware Security: A Hands-on Learning Approach*. Cambridge: Elsevier.

Burgstaller, Markus. 2005. *Theories of Compliance with International Law*. Leiden: Brill Academic.

Cimpanu, Catalin. 2020. 'Two More Cyber-Attacks Hit Israel's Water System.' ZDNet, 20 July. As of 21 October 2020: https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system

Council of Europe (CoE). 2004. Convention on Cybercrime, ETS 185.

Council of the European Union. 2008. *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical infrastructures and the assessment of the need to improve their protection*.

——— . 2017. *The Manual on Law Enforcement Information Exchange*. 6261/17, 4 July. As of 6 March 2021: https://data.consilium.europa.eu/doc/document/ST-6261-2017-INIT/en/pdf

Downs, George W., & Michael A. Jones. 2002. 'Reputation, Compliance, and International Law.' *Journal of Legal Studies* 31 (S1): S96.

Edison Electric Institute. 2018. 'Electric Distribution System Cybersecurity Is Critical in Today's Interconnected Society.' April. As of 25 October 2020: https://www.eei.org/issuesandpolicy/Documents/EEI_Cybersecurity_Considerations_Distribution.pdf

European Commission (EC). 2020. 'List of SPOCS & Competent authorities – NIS Directive.' As of 21 October 2020: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53682

European Union (EU). 2016. *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*.

European Union Agency for Cybersecurity (ENISA). 2009. 'Good Practices on Reporting Security Incidents.' December. As of 21 December 2020: https://www.enisa.europa.eu/publications/good-practice-guide-on-incident-reporting-1/at_download/fullReport

——— . 2019. *ENISA Threat Landscape Report 2018*. Athens: ENISA. As of 21 October 2020: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

——— . 2020a. 'Critical Infrastructures and Services.' As of 21 October 2020: https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services?tab=publications

——— . 2020b. *Sectoral/Thematic Threat Analysis: ENISA Threat Landscape*. Athens: ENISA. As of 21 October 2020: https://www.enisa.europa.eu/publications/sectoral-thematic-threat-analysis

——— . 2020c. *The Year in Review: ENISA Threat Landscape*. Athens: ENISA. As of 24 October: https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

Federal Ministry of the Interior, Germany. 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. Berlin: Government of Germany. As of 25 October: https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.html

Federal Office for Civil Protection, Switzerland. 2020. 'Critical Infrastructures.' As of 21 October 2020: https://www.babs.admin.ch/en/aufgabenbabs/ski/kritisch.html

Forum of Incident Response and Security Teams (FIRST). 2019. 'Information Exchange Policy 2.0 Framework Definition.' As of 21 October 2020: https://www.first.org/iep/iep_framework_2_0

———. 2020. 'Traffic Light Protocol (TLP): FIRST Standards Definitions and Usage Guidance – Version 1.0.' As of 21 October 2020: https://www.first.org/tlp

G-20. 2017. 'Communiqué – G20 Finance Ministers and Central Bank Governors Meeting.' Baden-Baden, Germany, 17–18 March 2017.

G-7. 2019. 'Cyber Norm Initiative Synthesis of Lessons Learned and Best Practices.' 26 August. As of 21 October 2020: https://www.diplomatie.gouv.fr/IMG/pdf/_eng_synthesis_cyber_norm_initiative_cle44136e.pdf

Gallagher, Ryan. 2020. 'Hackers "Without Conscience" Demand Ransom from Dozens of Hospitals and Labs Working on Coronavirus.' *Fortune*, 1 April. As of 21 October: https://fortune.com/2020/04/01/hackers-ransomware-hospitals-labs-coronavirus

Gavrilović, Andrijana. 2020. 'Confidence-Building Measures.' Geneva Internet Platform, February 2020. As of 21 October 2020: https://dig.watch/sessions/confidence-building-measures

Ghafur, Saira S. Kristensen, K. Honeyford, G. Martin, A. Darzi & P. Aylin. 2019. 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS.' *NPJ Digital Medicine* 98 (2).

Gisel, Laurent, & Lukasz Olejnik. 2019. *The Potential Human Cost of Cyber Operations*.

Geneva: International Committee of the Red Cross. As of 21 October 2020: https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf

Global Commission on the Stability of Cyberspace. 2019. *Advancing Cyberstability*. Final Report, November. As of 21 October 2020: https://cyberstability.org/wp-content/uploads/2020/02/GCSC-Advancing-Cyberstability.pdf

Global Cyber Security Capacity Centre. 2016. *Cybersecurity Capacity Maturity Model for Nations (CMM) – Revised Edition*. Oxford: University of Oxford. As of 21 October 2020: https://gcscc.ox.ac.uk/files/cmmrevisededition090220171pdf

Government of Australia. 2019. 'Australian Implementation of Norms of Responsible State Behaviour in Cyberspace.' As of 21 October 2020: https://www.dfat.gov.au/sites/default/files/how-australia-implements-the-ungge-norms.pdf

Government of Canada. 2019. 'Canada's Implementation of the 2015 GGE Norms.' As of 21 October 2020: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/11/canada-implementation-2015-gge-norms-nov-16-en.pdf

Government of the Netherlands. 2017. 'Building Digital Bridges: International Cyber Strategy.' 2 February. As of 21 October 2020: https://www.government.nl/documents/parliamentary-documents/2017/02/12/international-cyber-strategy

———. 2020. 'The Netherlands' Position Paper on the UN Open-ended Working Group "on Developments in the Field of Information and Telecommunications in the Context of International Security" and the UN Group of Governmental Experts "on Advancing responsible State behavior in cyberspace in the context of international security."' February. As of 21 October 2020: https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/letter-to-chair-of-oewg-kingdom-of-the-netherlands.pdf

Gusev, Alexey. 2020. 'New Cyberattacks Vectors of Russian Critical Infrastructure Enterprises: Domestic Private Banking Sector View within AI Protection Methods.' *Procedia Computer Science* 169: 314. As of 21 October 2020: https://www.sciencedirect.com/science/article/pii/S1877050920303124

Guzman, Andrew T. 2002. 'A Compliance Based Theory of International Law.' *California Law Review* 90(6): 1823. As of 21 October 2020: https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=1216&context=gjicl

Herzog, Stephen. 2011. 'Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses.' *Journal of Strategic Security* 4(2): 49.

IBM X-Force Incident Response and Intelligence Services. 2020. 'X-Force Threat Intelligence Index 2020'. February. As of 21 October 2020: https://www.ibm.com/security/digital-assets/xforce-threat-intelligence-index-map/#/

Ilves, Toomas Hendrik. 2007. 'Address by Toomas Hendrik Ilves President of the Republic of Estonia to the 62nd Session of the United Nations General Assembly (25 September 2007)'. As of 17 January 2021: https://www.un.org/webcast/ga/62/2007/pdfs/estonia-eng.pdf

Inter-American Committee Against Terrorism (CICTE). 2015. *Declaration: Protection of Critical Infrastructure from Emerging Threats*. CICTE document CICTE/doc.1/15, 23 March 2015. As of 21 October 2020: https://www.sites.oas.org/cyber/Documents/CICTE%20DOC%201%20DECLARATION%20CICTE00955E04.pdf

International Court of Justice (ICJ). 1997. *Gabčíkovo-Nagymaros Project (Hungary/Slovakia), Judgment, ICJ Reports 1997*, p. 7.

International Telecommunication Union (ITU). 2010. *Question 22-1: Securing Information and Communication Networks: Best Practices for Developing a Culture of Cybersecurity* (Final Report). Geneva: ITU. As of 25 October 2020: https://www.itu.int/pub/D-STG-SG01.22-2010

———. 2020. 'National Cybersecurity Strategies Repository.' As of 17 December 2020: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

———. 2021. 'CyberDrills.' As of 11 February 2021: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cyberdrills.aspx

ITU, The World Bank, Commonwealth Secretariat, the Commonwealth Telecommunications Organisation, NATO Cooperative Cyber Defence Centre of Excellence. 2018. *Guide to Developing a National Cybersecurity Strategy – Strategic Engagement in Cybersecurity*. Geneva: ITU.

INTERPOL. 2020. 'Preventing Crime and Protecting Police: INTERPOL's COVID-19 Global Threat Assessment.' April 6. As of 21 October 2020: https://www.interpol.int/en/News-and-Events/News/2020/Preventing-crime-and-protecting-police-INTERPOL-s-COVID-19-global-threat-assessment

Kaspersky ICS CERT. 2020a. 'Cyberthreats for ICS in Energy in Europe. Q1 2020.' As of 21 October 2020: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-2020Q1-Threats-to-energy-industry-in-Europe.pdf

———. 2020b. 'Threat landscape for industrial automation systems H1 2020'. September 24. As of 21 October 2020: https://ics-cert.kaspersky.com/media/KASPERSKY_H1_2020_ICS_REPORT_EN.pdf

———. 2021. 'Threat landscape for industrial automation systems. Statistics for H2 2020'. March 25. As of 28 March 2021: https://securelist.com/threat-landscape-for-industrial-automation-systems-statistics-for-h2-2020/101299/

———. Forthcoming. 'Threat Landscape for ICS in Water Management Industry.'

Khalili, Joel. 2020. 'Coronavirus Hospital Suspends Activity over Cyberattack.' *Techradar.Pro,* 16 March. As of 21 October 2020: https://www.techradar.com/news/coronavirus-hospital-suspends-activity-over-cyberattack

Lauber, Jurg. 2019. 'Chair's Summary: Informal Consultative Meeting of the Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security.' 5–6 December. As of 21 October 2020: https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf

Lee, Robert M., Michael J. Assante & Tim Conway. 2016. 'Analysis of the Cyber Attack on the Ukrainian Power Grid.' *SANS & E-ISAC*, 18 March. As of 21 October 2020: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

Maglaras, Leandros A., Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras & Tiago J. Cruz. 2018. 'Cyber Security of Critical Infrastructures.' *ICT Express* 4: 42–45.

Microsoft. 2020. 'Microsoft Digital Defense Report' September. As of 21 October 2020: https://www.microsoft.com/en-us/download/details.aspx?id=101738

Ministry of Europe and Foreign Affairs, France. 2018. 'Paris Call for Trust & Security in Cyberspace.' 11 December. As of 21 October 2020: https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf

Morse, Amyas. 2017. *Investigation: WannaCry Cyber Attack and the NHS*. London: National Audit Office. As of 21 October 2020: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs

Muthuppalaniappan, Menaka, & Kerrie Stevenson. 2020. 'Healthcare Cyber-Attacks and the COVID-19 Pandemic: An Urgent Threat to Global Health.' *International Journal for Quality in Health Care* 33 (1). As of 25 October 2020: https://academic.oup.com/intqhc/advance-article/doi/10.1093/intqhc/mzaa117/5912483

Nebenzia, Vassily. 2020. 'Statement by Vassily Nebenzia, Permanent Representative of the Russian Federation to the United Nations, at the "Arria-formula" VTC of the UNSC Members on Cyber-Attacks against Critical Infrastructure.' Permanent Mission of the Russian Federation to the United Nations, 26 August. As of 21 October 2020: https://russiaun.ru/en/news/arria_260820

Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security. 2020. 'Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security.' 27 May. As of 21 October 2020: https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf

———. 2021. 'Final Substantive Report.' 10 March 2021, UN Document A/AC.290/2021/CRP.2. As of 12 March 2021: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

Organisation for Economic Co-operation and Development (OECD). 2008a. 'Protection of "Critical Infrastructure" and the Role of Investment Policies Relating to National Security.' May. As of 21 October 2020: https://www.oecd.org/daf/inv/investment-policy/40700392.pdf

———. 2008b. *OECD Recommendation of the Council on the Protection of Critical Information Infrastructures*. OECD Document C(2008)35. Paris: OECD. As of 21 October 2020: http://www.oecd.org/sti/40825404.pdf

Organization for Security and Co-operation in Europe (OSCE) Permanent Council. 2013. 'Decision No. 1106: Initial Set of OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies.' OSCE Document PC.DEC/1106, 3 December 2013.

———. 2018. 'OSCE Holds National Table Top Exercise in Kazakhstan on Protecting Critical Energy Infrastructure from Cyber-Related Terrorist Attacks.' 29 November. As of 10 February 2021: https://www.osce.org/programme-office-in-astana/404594

Organization of American States (OAS). 2021. 'Cybersecurity Program.' As of 10 February 2021: http://www.oas.org/en/sms/cicte/prog-cybersecurity.asp

Permanent Mission of the Republic of Indonesia to the United Nations, New York. 2020. 'Statement by H.E. Ambassador Dian Triansyah Djani Permanent Representative of the Republic of Indonesia: United Nations Security Council Arria-formula Meeting "Cyber Stability, Conflict Prevention, and Capacity Building."' New York, 22 May. As of 21 October 2020: https://kemlu.go.id/newyork-un/en/read/united-nations-security-council-arria-formula-meeting-cyber-stability-conflict-prevention-and-capacity-building/3645/etc-menu

President's National Infrastructure Advisory Council (NIAC). 2017. 'Security Cyber Assets: Addressing Urgent Cyber Threats to Critical Infrastructure.' August. As of 21 October 2020: https://www.cisa.gov/sites/default/files/publications/niac-securing-cyber-assets-final-report-508.pdf p2

Republic of Mauritius. 2014. 'National Cyber Security Strategy 2014 – 2019.' As of 21 October 2020: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Mauritius_2014_National%20Cyber%20Security%20Strategy%20-%202014%20-%20EN.pdf

Schmidthaler, Michael, & Johannes Reichl. 2016. 'Assessing the Socio-Economic Effects of Power Outages Ad Hoc.' *Computer Science – Research and Development* 31: 157–61. As of 21 October 2020: https://link.springer.com/article/10.1007/s00450-014-0281-9

Security Magazine. 2020. 'Critical Infrastructure Cyberattacks a Greater Concern Than Enterprise Data Breaches.' *Security Magazine*, 26 March. As of 25 October 2020: https://www.securitymagazine.com/articles/91992-critical-infrastructure-cyberattacks-a-greater-concern-than-enterprise-data-breaches

Shanghai Cooperation Organization. 2009. 'Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization.' 16 June. As of 21 October 2020: http://eng.sectsco.org/load/207508/

Shea, Dana A. 2004. 'Critical Infrastructure: Control Systems and the Terrorist Threat.' CRS Report for Congress, RL31534, 20 January. As of 21 October 2020: https://apps.dtic.mil/sti/pdfs/ADA467307.pdf

Shuaia, Mao, Wang Chengzhib, Yu Shiwena, Gen Haoa, Yu Jufanga & Hou Hui. 2018. 'Review on Economic Loss Assessment of Power Outages.' *Procedia Computer Science* 130: 1158–63. As of 25 October 2020: https://www.sciencedirect.com/science/article/pii/S1877050918305131

Siemens Gas & Power. 2019. *Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?* Houston: Siemens. As of 21 October 2020: https://assets.new.siemens.com/siemens/assets/api/uuid:35089d45-e1c2-4b8b-b4e9-7ce8cae81eaa/version:1572434569/siemens-cybersecurity.pdf

Smith, Scott, Fabiola Sanchez & Christopher Torchia. 2019. 'Venezuela Buckles under Massive Power, Communications Outage.' *Associated Press*, 9 March. As of 21 October 2020: https://apnews.com/6ba2f69b77e2457da64593a7b8eced16

Statt, Nick. 2021. 'Hackers Tampered with a Water Treatment Facility in Florida by Changing Chemical Levels.' The Verge, 8 February. As of 8 February 2021: https://www.theverge.com/2021/2/8/22273170/hackers-water-treatment-facility-florida-hacked-chemical-levels-changed

Steffen, Sarah. 2016. 'Hackers Hold German Hospital Data Hostage.' DW, February 25. As of 21 October 2020: https://www.dw.com/en/hackers-hold-german-hospital-data-hostage/a-19076030

Suter, Manuel. 2007. *A Generic National Framework for Critical Information Infrastructure Protection (CIIP)*. Zurich: Center for Security Studies. As of 25 October 2020: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

United Nations Conference on International Organization. 1945. *Charter of the United Nations and Statute of the International Court of Justice*. San Francisco, 26 June.

United Nations Counter-Terrorism Committee Executive Directorate (UNCTED) & UN Office on Counter-Terrorism (UNOCT). 2018. *The Protection of Critical Infrastructures against Terrorist Attacks: Compendium of Good Practices*. June. As of 21 October 2020: https://www.un.org/sc/ctc/wp-content/uploads/2018/06/Compendium-CIP-final-version-120618_new_fonts_18_june_2018_optimized.pdf

United Nations General Assembly (UNGA). 1970. *Declaration on principles of international law concerning friendly relations and co-operation among States in accordance with the Charter of the United Nation*, UN Document A/PV.1883, 24 October 1970.

———. 1999. *Review of the implementations of the recommendations and decisions adopted by the General Assembly at its tenth special session: Report of the Disarmament Commission*, UN Document A/51/182/Rev.1, 9 June 1999. As of 21 October 2020: https://www.un.org/disarmament/wp-content/uploads/2019/09/A-51-182-Rev.1-E.pdf#page=53

———. 2001. *Responsibility of States for internationally wrongful acts*, UN Document A/RES/56/83, 28 January 2001.

———. 2010. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Document A/65/201, 10 July 2010.

———. 2015a. *Developments in the field of information and telecommunications in the context of international security*, UN Document A/RES/70/237, 23 December 2015.

———. 2015b. *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, UN document A/70/174, 22 July 2015.

United Nations Security Council (UNSC). 2017. UN document S/RES/2341 (2017), 13 February 2017.

United States Computer Emergency Readiness Team (US-CERT). 2015. 'US-CERT Federal Incident Notification Guidelines.' As of 6 March 2021: https://us-cert.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines_2015.pdf

United States Cybersecurity and Infrastructure Security Agency (CISA). 2020a. 'Alert (AA20-049A) Ransomware Impacting Pipeline Operations.' Department of Homeland Security, 18 February. As of 21 October 2020: https://us-cert.cisa.gov/ncas/alerts/aa20-049a

———. 2020b. 'Guidance on the Essential Critical Infrastructure Workforce: Ensuring Community and National Resilience in COVID-19 Response.' Version 4.0, 18 August. As of 11 February 2021: https://www.cisa.gov/sites/default/files/publications/ECIW_4.0_Guidance_on_Essential_Critical_Infrastructure_Workers_Final3_508_0.pdf

United States Department of Energy (DOE). 2019. *Evaluation Report*. DOE-OIG-20-12, 19 November. Washington, DC: US DOE. As of 25 October 2020: https://www.energy.gov/sites/prod/files/2019/11/f68/DOE-OIG-20-12.pdf

United States Department of Homeland Security. 2020. 'National Infrastructure Protection Plan International Issues for CI/KR Protection.' As of 25 October 2020: https://www.dhs.gov/xlibrary/assets/nipp_international.pdf

United States National Institute of Standards and Technology (NIST). 2012. *Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology*. Special Publication 800-61, Revision 2. Gaithersburg: US NIST. As of 25 October 2020: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Van der Vleuten, Erik, & Vincent Lagendijk. 2010. 'Transnational infrastructure vulnerability: The historical shaping of the 2006 European "Blackout."' *Energy Policy* 38 (4): 2042–2052.

Vidyarthi, Apratim, & Anastasiya Kazakova. 2020. 'What Cybersecurity Policymaking Can Learn from Normative Principles in Global Governance,' background paper, *IGF 2020 Best Practice Forum on Cybersecurity*, September 2020.

International Cooperation to Mitigate Cyber Operations against Critical Infrastructure

Normative Expectations and Emerging Good Practices

Malicious cyber operations pose a threat to critical infrastructure and thus to the well-being of our societies. Major incidents have the potential to both destabilize States and endanger international peace and security. To address the risk of increasingly complex and effective cyber threats aimed at critical infrastructure, the international community uses norms of expected behaviour of States in cyberspace to promote cooperation. This report investigates the norm – as proposed in 2015 by the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – that urges States to respond to other States' requests for assistance or mitigation in the event of malicious cyber operations against critical infrastructure.

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH