NORMS THROUGH SINGAPORE

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

NOVEMBER 2018

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

PROMOTING STABILITY IN CYBERSPACE TO BUILD PEACE AND PROSPERITY

The Global Commission on the Stability of Cyberspace (GCSC) will develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

www.cyberstability.org
info@cyberstability.org | cyber@hcss.nl
@theGCSC

***The Hague* Centre for Strategic Studies**
Lange Voorhout 1
2514 EA The Hague

info@hcss.nl
www.hcss.nl

EastWest Institute
New York | Brussels
Moscow | San Francisco

cyber@eastwest.ngo
www.eastwest.ngo

NORMS THROUGH SINGAPORE

CONTENTS

1. EXPLANATION OF THE NORM PACKAGE AND FOCUS OF THE GCSC

From its very beginnings, cyberspace has been designed in a decentralized manner, and therefore relatively loosely governed. This helped encourage the fledging technology and was likely critical for its rapid growth. Cyberspace has created unprecedented social and economic benefits, but it also created real risks and challenges for international peace and stability. While cyberspace is no longer the "Wild West," many nations still see it as an unconstrained arena for conflict. Dangerous actions by both state and non-state actors produce a growing sense of concern in the international community and the public at large.

These concerns have created widespread demand for better and more explicit governance structures for what has become an essential global infrastructure. Governance describes how individuals and both public and private institutions manage their shared interests and responsibilities. It can include both informal arrangements and formal institutions. Norms are foundational for agreement between stakeholders, better governance, and therefore the initial focus of our work. They also provide an apparent starting point for "what needs to be done" — a basic sense-test of what practical and operational steps need to be undertaken to achieve initial measures of "cyber stability" — and help us define what cyber stability actually is.

Accordingly, the Global Commission on the Stability of Cyberspace (GCSC) has approached its deliberations in a "bottom-up to top-down" manner. Firstly, the Commission is to identify operational norms that meet the most obvious urgent international cybersecurity needs as expressed by its members and which have not been addressed elsewhere.[1] Secondly, it will extrapolate from these and already existing norms a working definition of cyber stability and its underlying principles. Thirdly, it will use these principles to develop a clearer understanding of what the international peace and security architecture needs to do to meet that definition. Fourthly, it will offer recommendations to state and non-state stakeholders on how this can be accomplished. Taken together, the Commission aims to have a significant impact on the international peace and security architecture as it is relevant to cyberspace.

Throughout its deliberations, the GCSC is guided by significant shared core beliefs. These include the importance of a democratic, multi-stakeholder approach to governance, the necessity to promote development and economic growth, the need to balance rights and responsibilities for both states and individuals, and the centrality of cyberspace remaining open and unimpeded in its operations. We aim to expand the global understanding of responsible behavior in cyberspace in the context of international peace and security for both state and non-state actors.

We do not begin this work in a vacuum. Various stakeholder groups have identified possible norms and principles. These include the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security (UN GGE),[2] the G20,[3] the

1 The first two of these norms, the "Call to Protect the Public Core of the Internet" and the "Call to Protect Electoral Infrastructure," are enclosed in the final section of this report.

2 See, for example, the 2013 (*A/68/98*) and 2015 (*A/70/174*) Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE).

3 See G20 Leaders' Communiqué, Antalya Summit, 15-16 November 2015; G20 Leaders' Communiqué, Hangzhou Summit, 4-5 September 2016.

G7[4] and regional organizations,[5] as well as non-state norms developed by Microsoft[6] and ISOC,[7] to name but a few. It has also greatly benefited from the work done within the Internet governance ecosystem, including the work of the NETmundial Initiative[8] as well as the many initiatives occurring within the wider Internet Governance Forum (IGF) ecosystem.[9]

The GCSC's first task is therefore to examine how existing norms can be better supported and accompanied, where new norms are needed, and how to put these norms into operation and use. A norm works best when the international community is seized by it, when it shapes both the behavior of public and private institutions and the decisions of national leaders, and when it makes clear to all that some actions fall outside the bounds of what is acceptable.

There are precedents for our work. The Brundtland Commission created norms for Sustainable Development. A Carnegie Commission on Preventing Deadly Conflict led to the International Commission on Intervention and State Sovereignty and a commitment by all UN Member States on the duty to prevent and protect against war crimes, genocide, ethnic cleansing and other crimes against humanity. The Ilves Commission helped set the framework for the NETmundial Initiative. The Brandt and Palme Commissions represented important steps both in development and disarmament, respectively. These nongovernmental groups reshaped global discussion of responsible behavior and created new norms for unprecedented international problems.

We hope to do the same. While the UN GGE Reports have set a framework on the applicability of existing international norms, law and practices, we have sought to amplify and expand this initial normative structure in ways intended to complement and reinforce existing areas of agreement and point the way to new opportunities for increasing the stability of cyberspace. Our proposed norms are therefore intended to accompany and reinforce the eleven norms identified in the 2013-2015 UN GGE reports.

The norms developed both within and outside of the GCSC are foundational for our overall definition of cyber stability, as well as its guiding principles. First and foremost, these norms are based on the principle that no state or non-state actor should take actions that impair the stability of cyberspace, including inserting vulnerabilities into products and services, commandeering ICT devices to create botnets, and allowing non-state actors to conduct offensive cyber operations. Furthermore, the norms also urge state and non-state actors to take action when doing so is necessary to preserve the stability of cyberspace, including establishing vulnerabilities equities processes and enacting basic cyber hygiene. These norms are by necessity not complete. Instead, they provide an indication of what is needed to support the key principles of cyber stability. Other steps may be necessary as well.

4 See G7 Taormina Leaders' Communiqué, Taormina Summit, 26-27 May 2017.

5 Including but not limited to the work of ASEAN, AU, EU, OSCE and SCO.

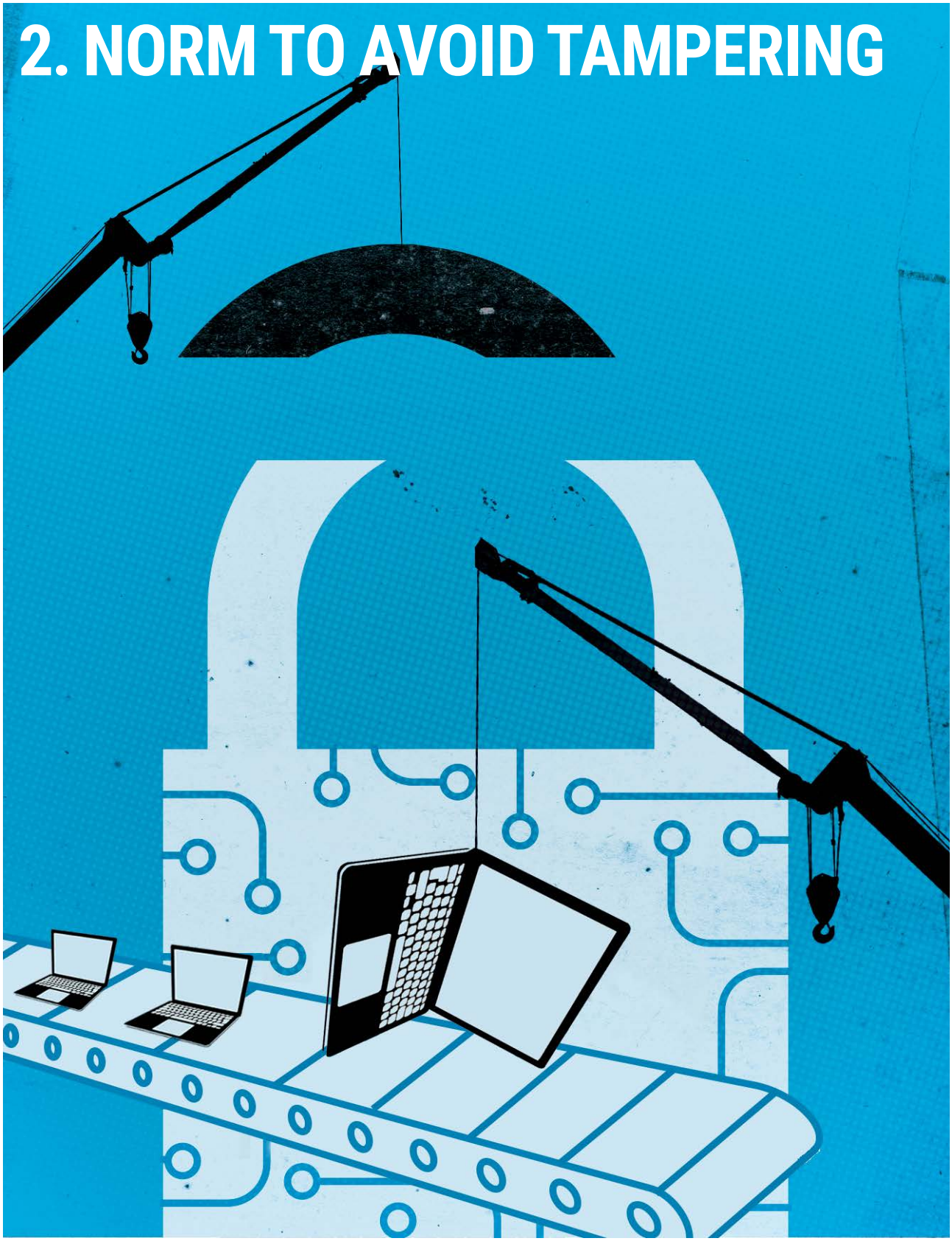
6 See, for example, Microsoft, International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVroA; The case for International Cybersecurity Norms, from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REY05a.

7 For example, MANRS, Mutually Agreed Norms for Routing Security, from https://www.manrs.org.

8 See the statement from the NETmundial Initiative here: http://netmundial.br/netmundial-multistakeholder-statement/

9 See, for example, the work of the IGF Best Practice Forum on Cybersecurity and the Dynamic Collation on Core Internet Values, to name but two examples.

2. NORM TO AVOID TAMPERING



NORM

"State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace."

BACKGROUND

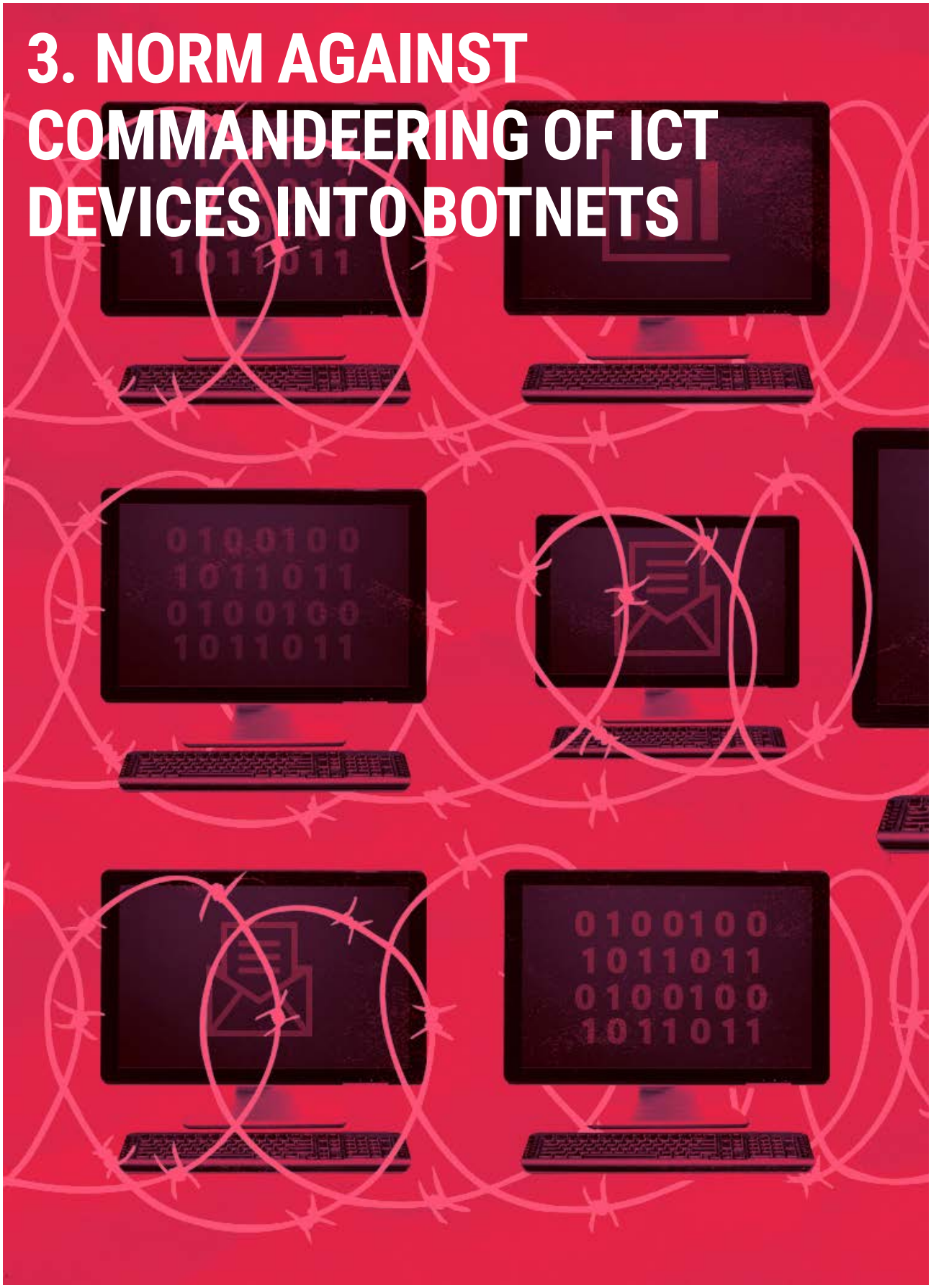
In a norm focused on "Non-Interference with the Public Core of the Internet," the Global Commission on the Stability of Cyberspace (GCSC) called upon state and non-state actors not to intentionally and substantially damage the general availability or integrity of the Public Core of the Internet. In support of this norm, the Commission noted the increasing dependence of other infrastructures on a stable and secure Internet and the potential dramatic consequences of its disruption. While the Public Core Norm focused on the "core of the Internet," individuals and organizations rely heavily upon certain commercial products to reach that Public Core and leverage the connectivity it provides. As a result, tampering with key components in software and hardware IT products (including, but not limited to, operating systems, Industrial Control Systems, switches, routers and other critical networking equipment, critical cryptographic products and standards, microchip design and widely used end-user consumer applications) may similarly deprive society of the ability to use and leverage the Internet safely and securely, and weaken overall the trust in its proper function. While such attacks are often in the news, what receives less attention is the fact that an attack can occur even before a product or its update reaches the market. For example, a product can be attacked by inserting a vulnerability — or secretly removing a security feature — during the design and manufacturing phase or during one of its updates. Put another way, a product can be tampered with prior to its release or production, with consequences for the public at large. The time between inserting a vulnerability, and activating the vulnerability for malicious use, can vary.

States have conflicting interests and responsibilities when dealing with information technology products. On the one hand, they have an obligation to promote the resilience and integrity of the cyber infrastructure to help thwart future cyber attacks by malicious actors and make the entire digital ecosystem safer. On the other hand, states have an obligation to their citizens to protect national security and combat criminals and other malicious actors in cyberspace. The exploitation of vulnerabilities in digital products and services used by adversaries has been leveraged by states to achieve their national security and public safety mission. Thus, to the extent that states consider exploiting vulnerabilities to be an effective approach to fulfilling their responsibilities, they may also find it helpful to intentionally introduce weaknesses or back doors into products and services used by adversaries. Non-state actors may in turn tamper with products and services as well, as their objectives may be aided by their ability to disrupt the stability of cyberspace.

It is important to note that the norm prohibits tampering a product or service line, which puts the stability of cyberspace at risk. This norm would not prohibit targeted state action that poses little risk to the overall stability of cyberspace; for example, the targeted interception and tampering of a limited number of end-user devices in order to facilitate military espionage or criminal investigations. This type of activity, unless it occurs within the basic infrastructure of the Public Core itself, or critically weakens user trust in the Internet globally, is unlikely to weaken the overall trust in cyberspace that is a condition of cyber stability. Although a non-state actor may also target systems in a limited way, such activity might violate existing criminal and civil laws.

While state and non-state actors should not affirmatively tamper with products in development or production, those in industry also have a responsibility to prevent such activities. Therefore, those creating products and services must commit to a reasonable level of diligence in the designing, developing and delivering of products and services that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities. Those concerned must also reject any apparent state or non-state efforts to compromise products and services, as well as adopt practices that reduce the risk of tampering and permit them to respond if tampering is discovered.

3. NORM AGAINST COMMANDEERING OF ICT DEVICES INTO BOTNETS



NORM

"State and non-state actors should not commandeer others' ICT resources for use as botnets or for similar purposes."

BACKGROUND

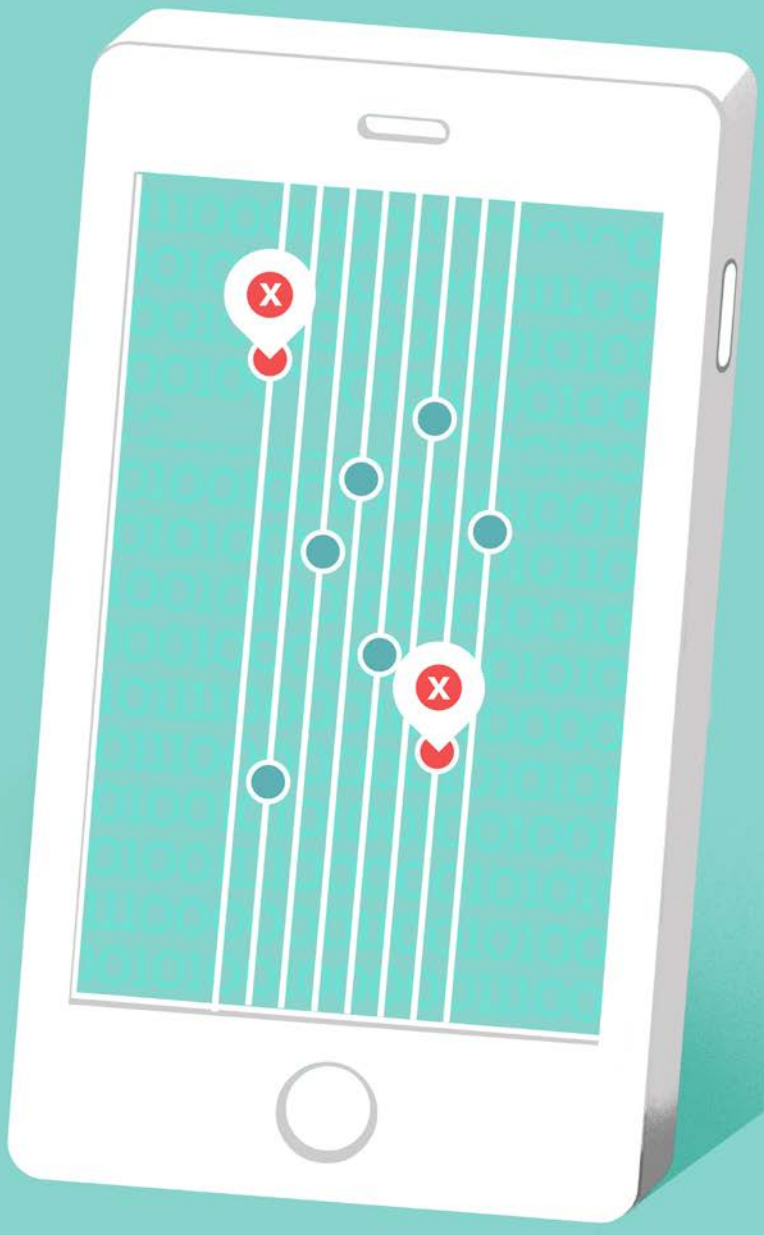
Internet-connected devices are becoming integral to people's lives globally. We are surrounded by devices with a multiplicity of computational, networking, sensing and actuating capabilities. Thermostats, televisions, medical devices, alarm clocks and automobiles have computing, storage and network capacity that can be appropriated and abused. Exploits of vulnerabilities in their underlying code can lead to physical safety issues for the individuals using the device: a device working outside of its design parameters could catch fire or create other unsafe conditions, such as unexpectedly unlocked doors, video broadcast from the interior of a house or cause (medical) equipment to fail.

We refer to botnets when software agents are installed, *en masse* and without consent, to use the devices' computational, storage or network resources. Those botnets can then be used to exercise direct effects on a different targeted system that can include impacting the end-targets' data confidentiality, availability and integrity. Therefore, a potentially uninvolved "third party" device, and its owner/operator, are made party to a malicious cyber activity without their knowledge. The compromise of devices to install malicious software agents not only weakens the defense of the device from other attacks — for instance from criminals — or infringes on the devices' normal functioning, but also casts the owner/operator as potentially culpable for damages inflicted on the end-target. This is particularly acute for cases where the compromise of the device might inadvertently cast the device and its owner/operator as an unwitting belligerent in interstate hostilities, and therefore invite reprisals or liability.

As we become reliant on technology in our personal environment, and more and more connected devices enter the market, the exploitation of consumer devices and their use as botnets increasingly undermines trust and destabilizes society. The Commission recognizes that there are cases — for instance for law enforcement purposes — in which authorized state actors may find it necessary to install software agents on devices of a specifically targeted individual adversary, or a group of adversaries. However, state and non-state actors should not commandeer civilian devices of the general public (*en masse*) to facilitate or directly execute offensive cyber operations, irrespective of motivation. [10]

10 This norm is complementary to the previous proposed norm for state and non-state actors to avoid tampering with products prior to their release, which focuses on supply chain aspects, while this norm looks at already deployed devices.

4. NORM FOR STATES TO CREATE A VULNERABILITY EQUITIES PROCESS



NORM

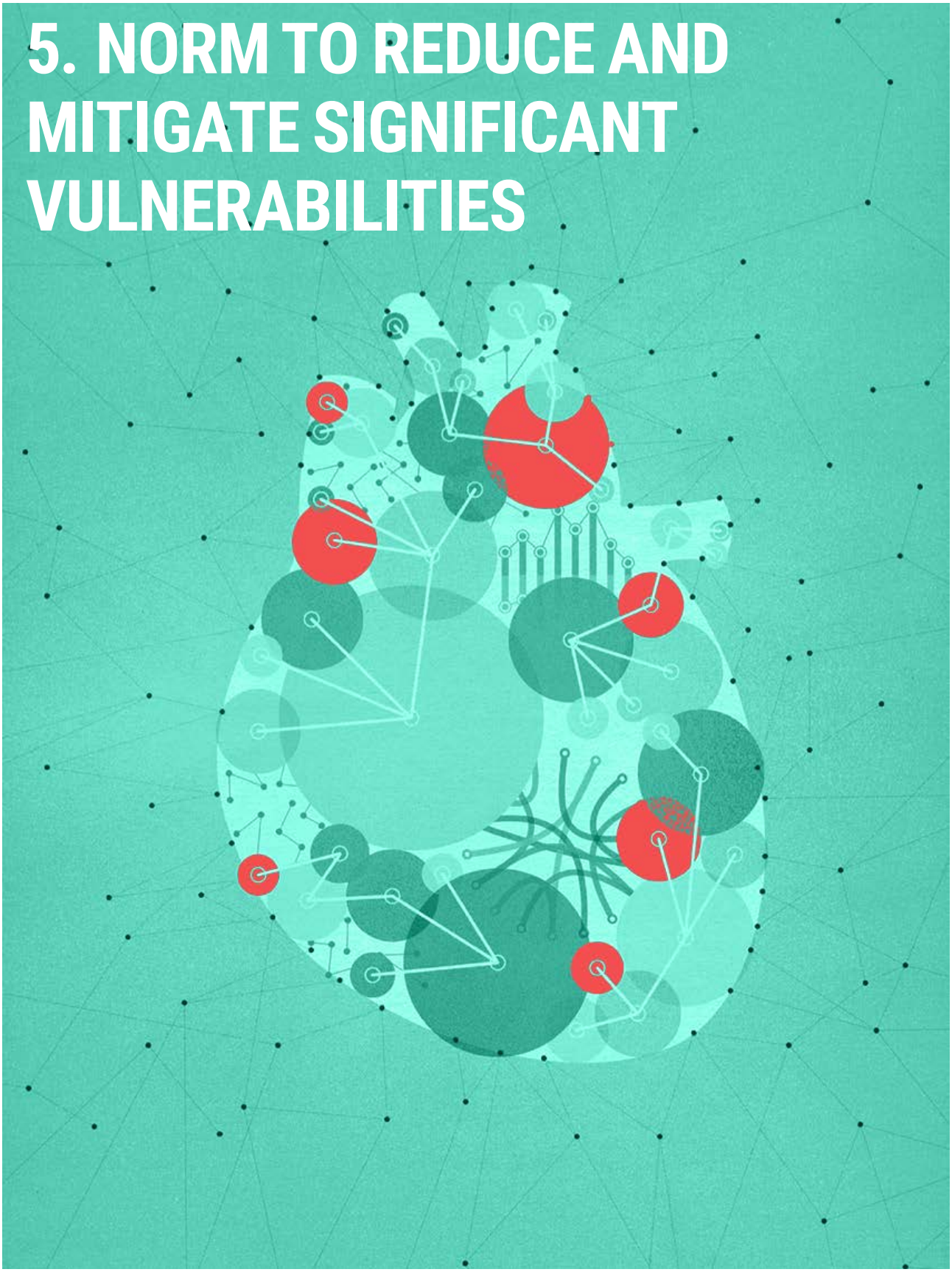
"States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure."

BACKGROUND

As the complexity of operating systems, critical software and computer hardware grows, they increasingly contain vulnerabilities. Those vulnerabilities can be exploited by state and non-state actors. States sometimes have conflicting interests and responsibilities when dealing with newly discovered vulnerabilities. On the one hand, they have an obligation to promote the resilience and integrity of infrastructure essential to the stability of cyberspace and by helping thwart malicious cyber activity make the entire digital ecosystem safer for all users. This would argue for a state to quickly disclose newly discovered vulnerabilities to vendors and manufacturers for patching, as well as making broader public disclosures, where appropriate, to protect the public. On the other hand, states have an obligation to protect their citizens from criminals, to investigate and prosecute cyber crime offenses, and reserve the right to impose sanctions that act as both a specific and a general deterrent to future malicious activity. An essential tool to pursue malicious actors, and particularly sophisticated actors such as rogue states, is the exploitation of computer code vulnerabilities in the digital infrastructure on which they rely. States therefore often argue that they must preserve at least some select capabilities, including the use of undisclosed vulnerabilities, or else extremely capable malicious actors would go undiscovered and unchecked.

While states are unlikely to voluntarily disclose every vulnerability they discover, there has been a recent move by several states away from a presumption that all vulnerabilities will be retained, to one where the presumption is in favor of disclosure in the interests of greater systemic cybersecurity. A key part of this is the creation, by states, of a publicly described process for assessing the pros and cons of disclosure that takes into account the full range of policy, economic, social and technical equities. More specifically, that process should be procedurally transparent and take into account a full range of views including factors such as: network security and resiliency; the security of users and their data; law enforcement and national security utility; and diplomatic and commercial implications. The United States has recently promulgated a new version of such a process and other countries are considering creating their own Vulnerability Equities Process (VEP) policies. Given that vulnerability discovery and disclosure is broader than any one state, in order to promote network resilience while at the same time safeguarding national security, it would be in the interest of the long-term stability of cyberspace for every state to have such a process in place. Additionally, states should work towards compatible and predictable processes. The existence of such processes can act as a confidence-building measure between states in that it provides some assurance that relevant equities and competing interests are fully considered. Of course, every state has differing capabilities and unique interagency structures, however, any effective VEP process should be designed to take a broad range of perspectives and equities into account. In addition, though the actual decisions reached in individual cases may, out of necessity, remain confidential, there should be transparency on the general procedures and framework for reaching such decisions. Finally, this norm deals only with the establishment of a process where disclosure decisions are made. If a government or any other entity decides to make a disclosure, such disclosure should be made in a responsible manner that promotes public safety and does not lead to exploitation of that vulnerability.

5. NORM TO REDUCE AND MITIGATE SIGNIFICANT VULNERABILITIES



NORM

"Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on vulnerabilities in order to help prevent or mitigate malicious cyber activity."

BACKGROUND

Certain IT products and services are essential to the stability of cyberspace due to their use within the core technical infrastructure, such as in core name resolution or routing, because of their widespread facilitation of the user Internet experience, or their criticality to the functioning of critical infrastructures such as election systems or power generation. Those creating products and services must commit to a reasonable level of diligence in the designing, developing, and delivering of products and services that prioritizes security and in turn reduces the likelihood, frequency, exploitability and severity of vulnerabilities.

Due to the increasing complexity of software and hardware, vulnerabilities in those products are a fact of life. While those vulnerabilities are usually unintentional, malicious state and non-state actors often exploit these vulnerabilities when discovered in ways that undermine the stability of cyberspace.

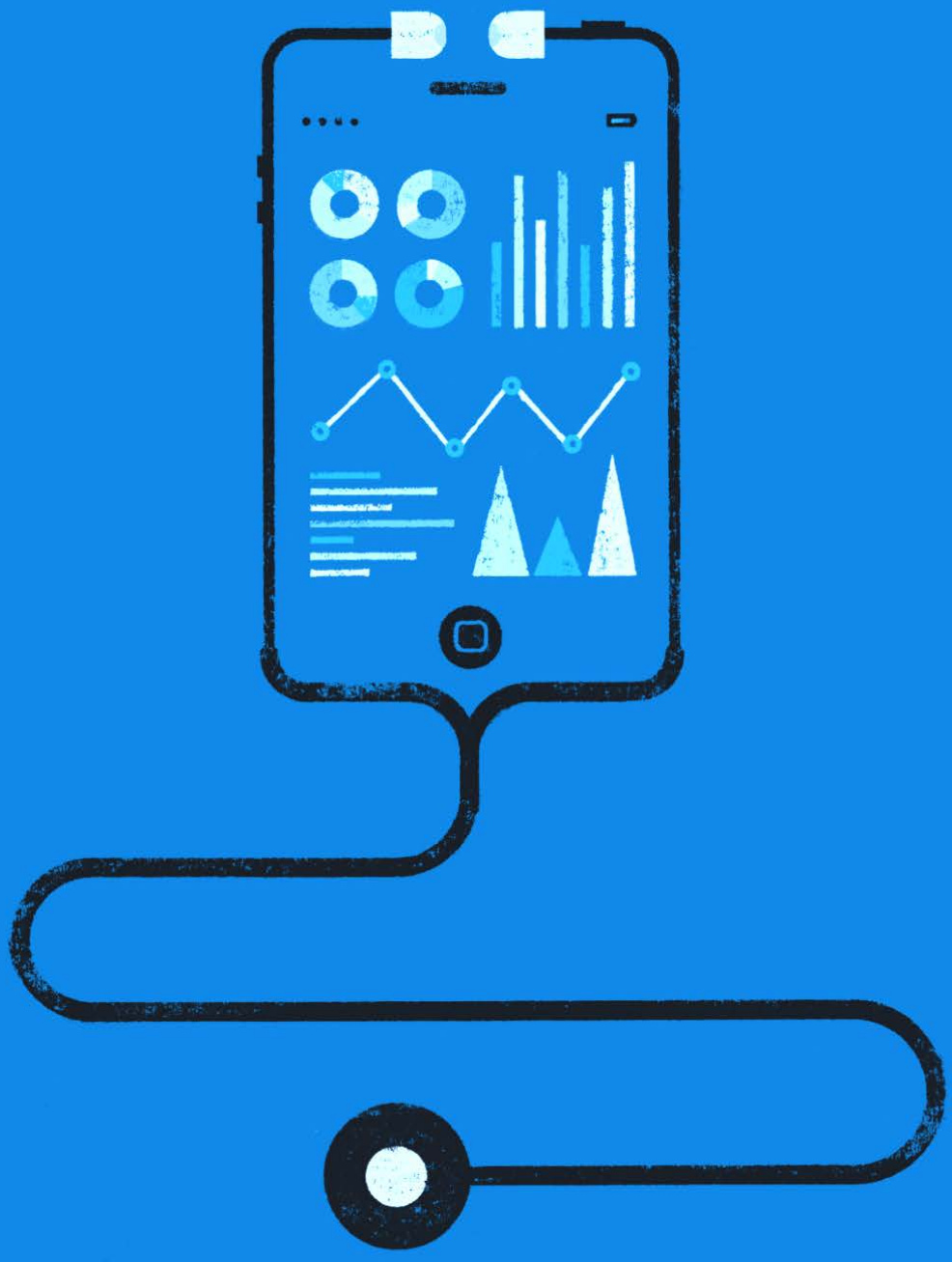
Moreover, in a hyper-connected and hyper-dependent world a discovered vulnerability may affect multiple products and services by different producers and in different environments. Patching one product without disclosing the underlying vulnerability to others may protect that product but not protect the stability of cyberspace writ large. Those in the best position to assess the impact of a given vulnerability are often those who develop, produce, install or operate the products that the vulnerabilities affect. It is important to share information that would assist in fixing security vulnerabilities or help prevent, limit or mitigate an attack.[11]

While it is currently very difficult to ensure that no vulnerabilities exist in newly released or updated products, rather, this proposed norm suggests that those involved in the development or production of such products take "reasonable steps" that would reduce the frequency and severity of those that do occur.

Just as the "no tampering" norm addresses intentional insertion of vulnerabilities into critical products and services, and the hygiene norm ultimately addresses the duties of end users, this proposed norm seeks to have those who develop or produce critical products take reasonable measures to ensure that the number and scope of critical vulnerabilities are minimized and that they are effectively and timely mitigated and, when appropriate, disclosed when discovered. The process used should be transparent to create a predictable and stable environment.

11 One of the norms for responsible behavior of states in the 2015 Report of the UN GGE (*A/70/174*) affirms that "States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure."

6. NORM ON BASIC CYBER HYGIENE AS FOUNDATIONAL DEFENSE



NORM

"States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene."

BACKGROUND

As Internet connectivity spreads around the world pervading all aspects of modern life, users of every kind — individuals, organizations, enterprises, and governments — are growing more and more reliant on technology and access to information available on the Internet. Politics, economics, public information, education, development and every other manner of social interaction depend critically on the Internet and associated technologies. Yet, this modern wonder remains broadly unsafe, and no one is immune to its dangers.

Consensus has yet to emerge on the most effective ways to optimize the promising technologies of cyberspace while safeguarding the public. Yet, most agree that the benefits of our digitally-connected lives cannot be sustained going forward without agreed standards of essential security in cyberspace. To this end, the Commission strongly endorses the widespread adoption and verified implementation of basic cyber hygiene — a regime of foundational measures that represent prioritized, essential tasks to perform to defend against, prevent and rapidly mitigate avoidable dangers in cyberspace. Indeed, given the extensiveness of interconnectivity online, these measures constitute a basic duty of care that should be required of all users. Hygiene regimes should incorporate reliable measures of implementation, provide for widespread sharing of technical information and best practices, and be subject to appropriate oversight. Increasingly smart devices and processes demand smart laws and regulations. In creating more accountability for this basic duty of cyber care, governments should not curtail innovation or confound with the basic properties of the Internet.

Cyber hygiene standards already exist in various forms.[12] They have been gaining wider international acceptance, as governments and enterprises increasingly understand the importance of taking steps demonstrated to help prevent and rapidly mitigate the dangers of known malware. Moreover, these standards represent best practice, highlight the importance of sensible, regular oversight and underscore the importance of automated information sharing where possible to alert other users to trouble. Such basic cyber defenses as outlined in these approaches account for the reality that no government, organization or collection of users can single-handedly alleviate all cyber-related risks. They also recognize that users at every level have important roles to play in strengthening cybersecurity.

The Global Commission on the Stability of Cyberspace believes that fundamental cybersecurity defense through the widespread adoption of cyber hygiene has become essential to the responsible use and beneficial growth of the Internet. Security must be seen as a continuous process with responsibilities distributed among all actors with mechanisms in place, such as automated reporting and information sharing, to ensure appropriate accountability.

The Commission also recognizes that many societies around the world face considerable challenges in the use of information and communications technologies and calls on states to share knowledge and offer capacity building to instantiate processes for the effective implementation of basic cyber hygiene regimes to widen the effect of this norm.

12 This includes, for example, by the European Telecommunications Standards Institute (ETSI), the not-for-profit Center for Internet Security (CIS) and the Australian Signals Directorate (ASD), among others.

7. NORM AGAINST OFFENSIVE CYBER OPERATIONS BY NON-STATE ACTORS

NORM

"Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur."

BACKGROUND

While information and communication technologies have positively transformed societies, they also pose new security challenges. The speed and ubiquity of cyber operations often poses considerable difficulties to states' judicial systems and international law enforcement cooperation. Despite these difficulties, it should be recalled that state sovereignty is the cornerstone of the rules-based international system of peace and security. States have a monopoly on the legitimate use of force, strictly bound by international law. Some non-state actors, mainly private companies, advocate for the right to conduct offensive cyber operations across national borders, potentially claiming that it constitutes "self defense" as states do not have the capacity to adequately protect them against cyber threats. These non-state actors' offensive cyber operations are sometimes euphemistically referred to as "active cyber defense,"[13] including but not limited to so-called "hack-back," as they are conducted for defensive purposes.

Some states are unable to control — or chose to actively ignore — these practices, despite the risk they impose upon the stability and security of cyberspace. However, in most states such practices would be unlawful, if not criminalized, while in other states they appear to be neither prohibited nor explicitly authorized. A few states are, nevertheless, considering legitimizing non-state actors' offensive cyber operations. Indeed, some have decided or proposed legislation to allow offensive operations by non-state actors in their domestic legislation.

The Global Commission on the Stability of Cyberspace believes that these practices undermine the stability of cyberspace. They can result in serious disruption and damages, including for third parties, and are thus likely to trigger complex international legal disputes and escalate conflicts. States explicitly granting or knowingly allowing non-state actors the authorization to conduct offensive operations, for their own purposes or those of third parties, would set a dangerous precedent and would breach international law in most cases. The Commission believes that offensive measures should be reserved solely to states and recalls that international law establishes a strict and exclusive framework for international response to hostile acts that also applies to cyber operations. Similarly, under international law, non-state actors acting on behalf of states must be considered their agents and are therefore considered extensions of the state.[14]

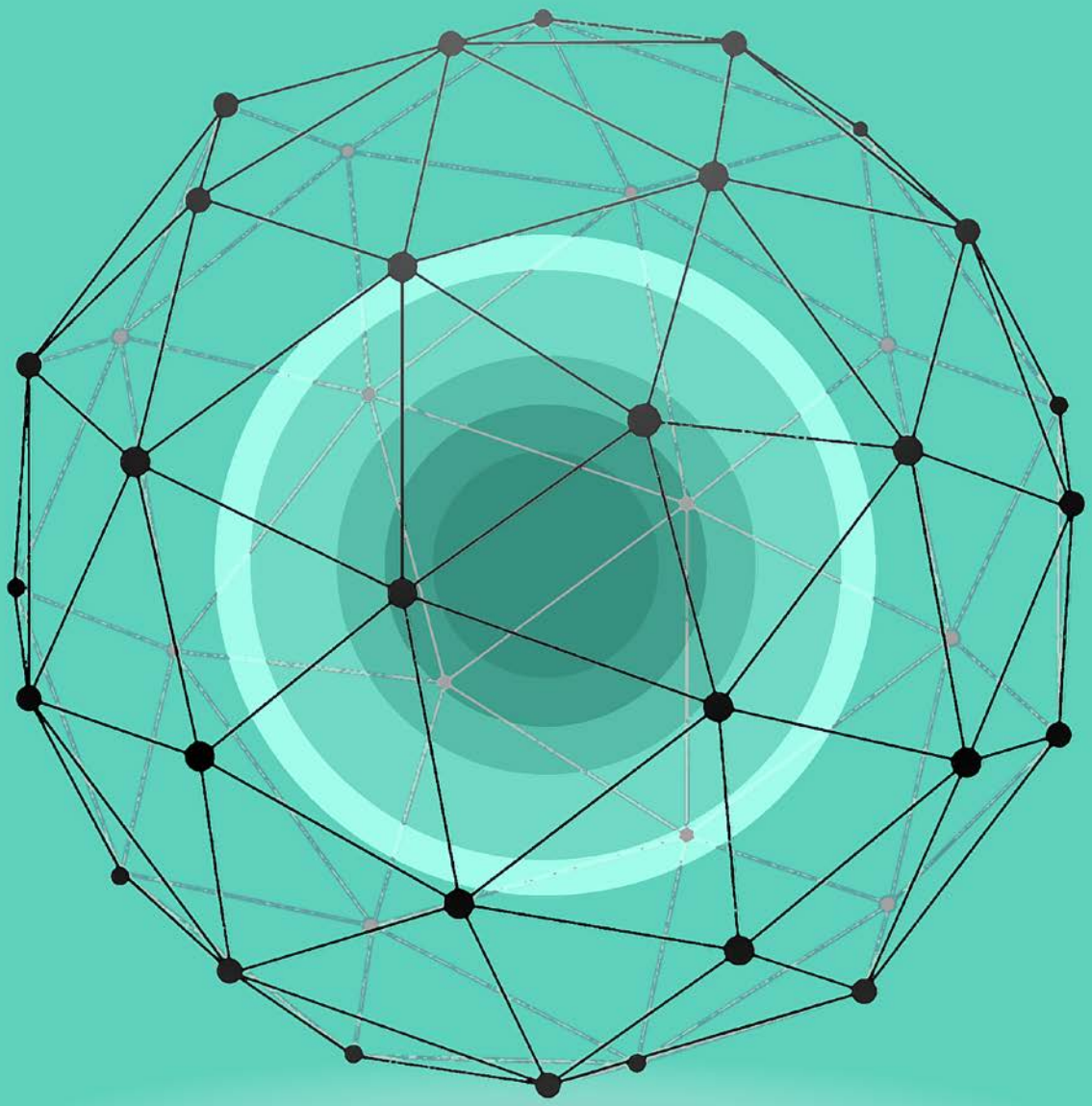
If states permit such action, they may therefore be held responsible under international law.[15] States must act, domestically and internationally, to prevent offensive cyber operations by non-states actors.

13 Active cyber defense should be understood as a set of measures ranging from self defense on the victim's network to destructive activity on the attacker's network. Offensive cyber operations within this continuum imply for the defender to act outside of its own network independently of their intention (offense or defense) and the legal qualification of their acts. Further work should be conducted on the definition of offensive cyber operations and active cyber defense.

14 See "additional note" for a wider treatment of the case within international law, available here: https://cyberstability.org/wp-content/uploads/2018/11/Additional-Note-to-the-Norm-Against-Offensive-Cyber-Operations-by-Non-state-Actors-Norm-Package-Singapore.pdf.

15 Ibid.

8. PREVIOUSLY RELEASED NORMS



CALL TO PROTECT THE PUBLIC CORE OF THE INTERNET

New Delhi, November 2017

NORM

> **Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.[16]**

BACKGROUND

The Internet has changed the world, fueling political, economic, and social growth. More generally, cyberspace promotes communication, commerce, education, human rights and livelihood on every level. To continue this progress, we believe that the stability of cyberspace is essential for the good of humanity now and into the future.

As with all critical infrastructures, the technology that underpins the global Internet is imperfect. Technology can break, and the existence of flaws, vulnerabilities, malicious actors and the development of offensive capabilities create conditions of instability that put the benefits of cyberspace in jeopardy.

The Global Commission on the Stability of Cyberspace was established to enhance international peace, security, and stability by proposing norms and initiatives to guide responsible state and non-state behavior in cyberspace. A commitment to norms, together with the application of international law, can significantly enhance cyber stability.[17]

As a first step, recognizing the global reliance on cyberspace, the increasing dependence of other infrastructures on its reliability, and the potentially dramatic consequences of its disruption, the Commission urges all stakeholders to adhere to the following norm that sustains the general availability and integrity of the Internet.

16 Elements of the public core include, inter alia, Internet routing, the domain name system, certificates and trust, and communications cables, which have been further defined in the ***Definition of the Public Core, to which the norm applies***.

17 Norms are voluntary, non-binding commitments. Over time they can crystallize into international law. Norms prescribe a positive or a negative obligation. The overall stability of the cyberspace is also served through capacity and confidence building efforts.

DEFINITION OF THE PUBLIC CORE, TO WHICH THE NORM APPLIES

Bratislava, May 2018

In November, 2017, the Global Commission on the Stability of Cyberspace (GCSC) issued its *Call to Protect the Public Core of the Internet*:

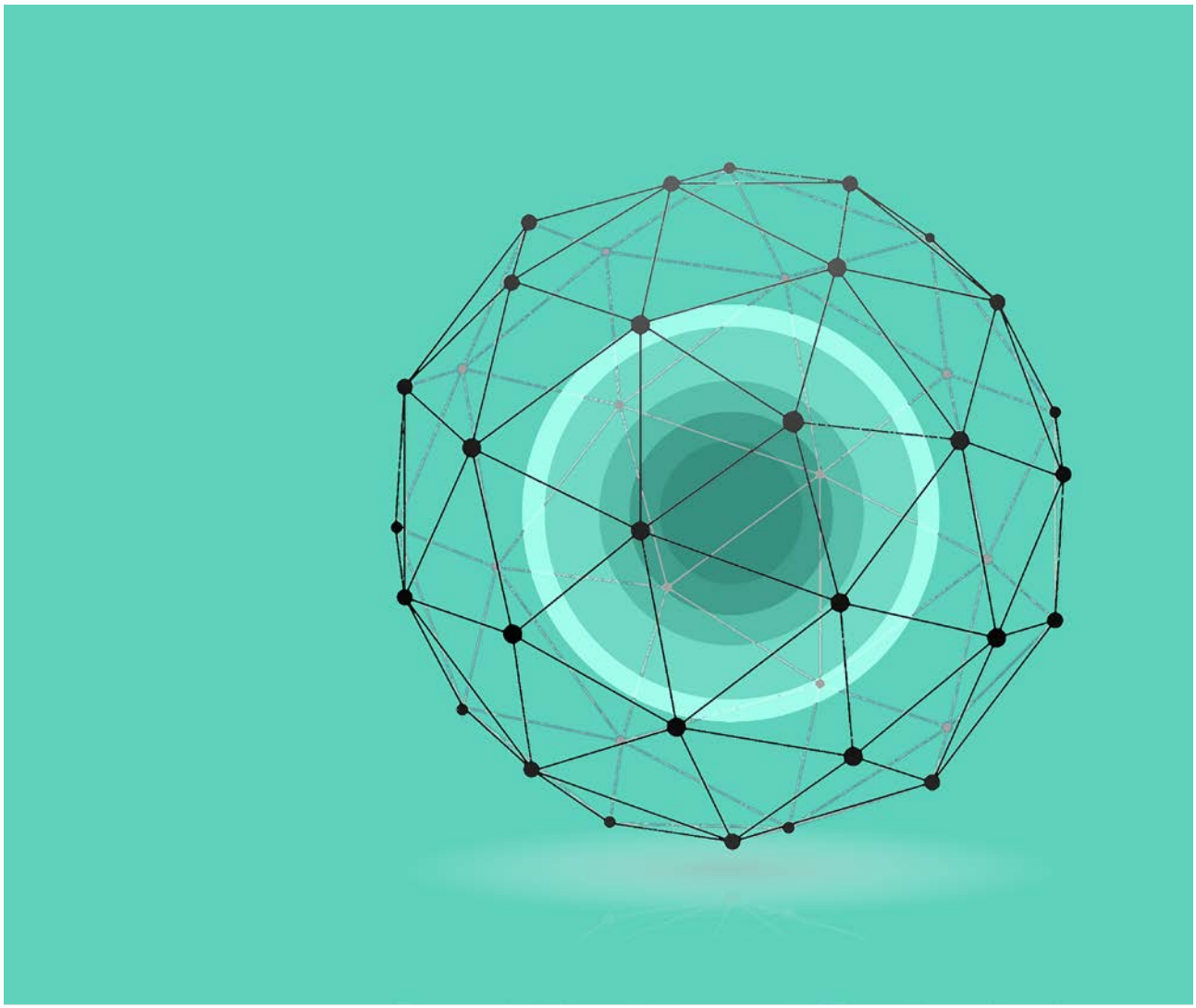
> ## NON-INTERFERENCE WITH THE PUBLIC CORE
>
> **Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.**

As input to its process, a working group of the GCSC conducted a broad survey of experts on communications infrastructure and cyber defense to assess which infrastructures were deemed most worthy of protection. On a scale of zero to ten, with zero being "unworthy of special protection" and ten being "essential to include in the protected class," all surveyed categories ranked between 6.02 and 9.01. Accordingly, the Commission defines the phrase "the public core of the Internet" to include packet routing and forwarding, naming and numbering systems, the cryptographic mechanisms of security and identity, and physical transmission media. Specifically:

Packet routing and forwarding include, but are not limited to: the equipment, facilities, information, protocols, and systems which facilitate the transmission of packetized communications from their sources to their destinations. This includes Internet Exchange Points (the physical sites where Internet bandwidth is produced) and the peering and core routers of major networks which transport that bandwidth to users. It includes systems needed to assure routing authenticity and defend the network from abusive behavior. It includes the design, production, and supply-chain of equipment used for the above purposes. It also includes the integrity of the routing protocols themselves and their development, standardization, and maintenance processes.

Naming and numbering systems include, but are not limited to: systems and information used in the operation of the Internet's Domain Name System, including registries, name servers, zone content, infrastructure and processes such as DNSSEC used to cryptographically sign records, and the whois information services for the root zone, inverse-address hierarchy, country-code, geographic, and internationalized top level domains and for new generic and non-military generic top-level domains. It includes frequently used public recursive DNS resolvers. It includes the systems of the Internet Assigned Numbers Authority and the Regional Internet Registries which make available and maintain the unique allocation of Internet Protocol addresses, Autonomous System Numbers, and Internet Protocol Identifiers. It also includes the naming and numbering protocols themselves and the integrity of the standardization processes and outcomes for protocol development and maintenance.

The cryptographic mechanisms of security and identity include, but are not limited to:



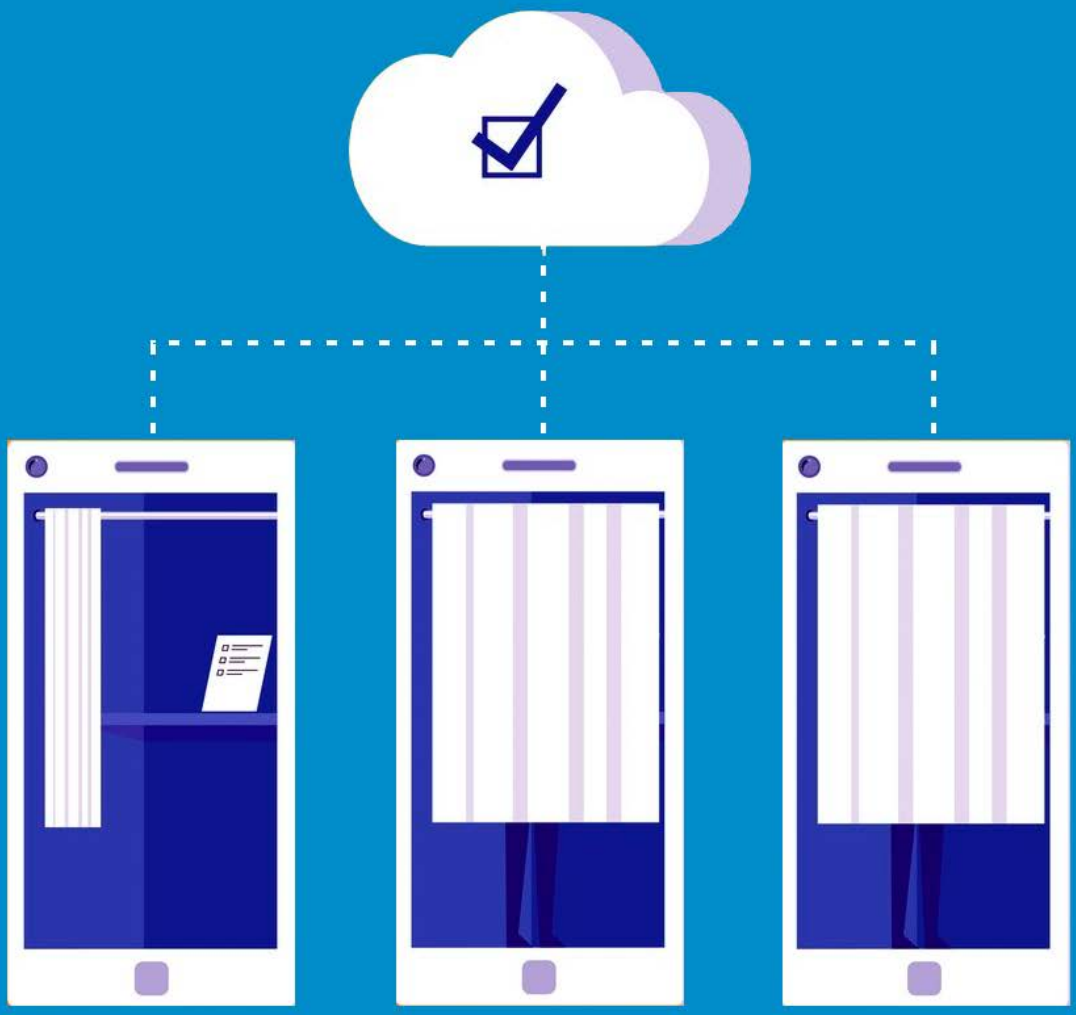
the cryptographic keys which are used to authenticate users and devices and secure Internet transactions, and the equipment, facilities, information, protocols, and systems which enable the production, communication, use, and deprecation of those keys. This includes PGP keyservers, Certificate Authorities and their Public Key Infrastructure, DANE and its supporting protocols and infrastructure, certificate revocation mechanisms and transparency logs, password managers, and roaming access authenticators. It also includes the integrity of the standardization processes and outcomes for cryptographic algorithm and protocol development and maintenance and the design, production, and supply-chain of equipment used to implement cryptographic processes.

Physical transmission media include, but are not limited to: physical cable systems and installations for wired communications serving the public, whether fiber or copper. This includes terrestrial and undersea cables and the landing stations, datacenters, and other physical facilities which support them. It includes the support systems for transmission, signal regeneration, branching, multiplexing, and signal-to-noise discrimination. It is understood to include cable systems that serve regions or populations, but not those that serve the customers of individual companies.

Some experts believe that far more categories of Internet and ICT-enabled infrastructure are deserving of protection, so this definition may be broadened in the future.

CALL TO PROTECT THE ELECTORAL INFRASTRUCTURE

Bratislava, May 2018



NORM

State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites.

BACKGROUND

Of all the rules, precepts and principles that guide the conduct of states in the comity of nations, the norm of non-interference is perhaps held most sacred. Article 2(4) of the United Nations Charter articulates this norm and elevates it as a principle of legal, and thus, binding character:

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*

Through this provision, the framers of the Charter acknowledged that the gravest threats to the principle of non-intervention came from coercive measures directed at a state's physical or political autonomy, as, indeed, both are essential to state sovereignty. The territory controlled by a state may be a manifestation of its sovereign capacity, but it is worthless without the enjoyment of political agency and independence. Moreover, nothing reflects genuine political independence more than national participatory processes, such as elections, conducted freely and fairly. The UN Charter sought to grant strong protections against undue external interference. Those protective measures have now come to be challenged again in the digital age.

The advent of the Internet and the accompanying wave of "digitalisation" has opened up new opportunities for the material, cultural and intellectual advancement of communities across the world. But it has also pried open the possibility of malicious actors—acting alone, collectively, or on behalf of states— manipulating elections through digital means. With national participatory processes becoming more complex in scale and sophistication, there has been a burgeoning of data, institutions and infrastructure to manage them. Many countries today publish their electoral rolls—a basic, traditional guarantee against voting manipulation or fraud—online, exposing such databases to cyber attacks and exploitation. Similarly, electoral voting instruments are used in far flung and remote areas of a country, where its operators are not fully abreast of the risks and concerns associated with their digital manipulation. Voting software suppliers and computer systems at the local or "booth" levels remain susceptible to such intrusions as well.

Seized of the growing number and intensity of threats to participative processes, the Global Commission on the Stability of Cyberspace recommends stronger national measures and effective international cooperation to prevent, mitigate and respond to cyber intrusions against the technical electoral infrastructure. The Commission acknowledges that the actual conduct of elections or participatory processes at the regional, local or federal level is firmly the remit of states, to be carried out in accordance with their respective national laws. Nevertheless, the cyber attacks on their electoral infrastructure may originate from outside the borders, necessitating multilateral cooperation resolution. As more countries opt to digitise their election machinery, the risks and vulnerabilities associated with such infrastructure increase manifold, as does the prospect of a major, offensive cyber operation. A modest first step to effective multilateral cooperation would be a pledge or commitment from governments to refrain from engaging in cyber operations against the technical electoral infrastructure of another state. In recommending this norm, the Commission merely affirms the numerous international legal protections already afforded against external interference in the internal affairs of another state.

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org | info@cyberstability.org | cyber@hcss.nl | @theGCSC

CHAIRS

Michael Chertoff USA
Latha Reddy India

COMMISSIONERS

Abdul-Hakeem Ajijola Nigeria
Virgilio Almeida Brazil
Isaac Ben-Israel Israel
Scott Charney USA
Frédérick Douzet France
Anriette Esterhuysen South Africa
Jane Holl Lute USA
Nigel Inkster UK
Marina Kaljurand Estonia
Khoo Boon Hui Singapore
Wolfgang Kleinwächter Germany
Olaf Kolkman Netherlands
Lee Xiaodong China
James Lewis USA
Jeff Moss USA
Elina Noor Malaysia
Joseph S. Nye, Jr. USA
Christopher Painter USA
Uri Rosenthal Netherlands
Ilya Sachkov Russia
Samir Saran India
Marietje Schaake Netherlands
Motohiro Tsuchiya Japan
Bill Woodcock USA
Zhang Li China
Jonathan Zittrain USA

SPECIAL REPRESENTATIVES AND ADVISORS

Carl Bildt Sweden
Vint Cerf USA
Sorin Ducaru Romania
Martha Finnemore USA

DIRECTORS

Alexander Klimburg Austria
Bruce W. McConnell USA

RESEARCH ADVISORY GROUP CHAIRS

Sean Kanuck USA
Koichiro Komiyama Japan
Marilia Maciel Brazil
Liis Vihul Estonia
Hugo Zylberberg France

GLOBAL COMMISSION
ON THE STABILITY OF CYBERSPACE

www.cyberstability.org
info@cyberstability.org
cyber@hcss.nl
@theGCSC

SECRETARIAT

The Hague Centre for Strategic Studies

EastWest INSTITUTE

PARTNERS

Ministry of Foreign Affairs of the Netherlands

CSA SINGAPORE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES

Internet Society

Microsoft

Afilias

SPONSORS

Ministry of Foreign Affairs of Estonia
GLOBSEC
Ministry of Internal Affairs and Communications of Japan
UNIDIR
Federal Department of Foreign Affairs of Switzerland

SUPPORTERS

Black Hat USA
Packet Clearing House
Tel Aviv University
European Union Delegation to the UN in Geneva
DEF CON