Our submission to The Global Commission on the Stability of Cyberspace's Request for Consultation on the Norm Package Singapore

About Global Partners Digital

The advent of the internet – and the wider digital environment – has enabled new forms of free expression, organisation and association, provided unprecedented access to information and ideas, and catalysed rapid economic and social development. It has also facilitated new forms of repression and violation of human rights, and intensified existing inequalities. Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values. We do this by making policy spaces and processes more open, inclusive and transparent, and by facilitating strategic, informed and coordinated engagement in these processes by public interest actors.

Our submission/output

GPD welcomes the opportunity to respond to the Global Commission on the Stability of Cyberspace's (GCSC) Request for Consultation (RFC) on the proposed norms of the Norm Package Singapore, issued by the GCSC in November 2018. Our submission to the RFC is premised on the mutually reinforcing and interdependent relationship between the promotion, protection and enjoyment of human rights and the security and stability of cyberspace. This means norms and policies that promote a secure and stable cyberspace also protect and promote human rights. As such any measures which undermine the rights of end-users also risk undermining the security and stability of cyberspace. In addition, due to the nature of cyberspace itself, which has been developed and continues to evolve and function as a result of the involvement of a broad range of stakeholders, a secure and stable cyberspace requires the inclusive engagement and cooperation of stakeholders. The need for holistic and inclusive approaches has only become more urgent with the increase in frequency, scale and complexity of cyberthreats and cyberattacks. Sustainable and responsive solutions to these cybersecurity challenges therefore necessitate inclusive, holistic, expert-driven approaches that engage a broad range of stakeholders.

Our feedback on the Norm Package Singapore suggests amendments which promote the mutually reinforcing and interdependent relationship between human rights and the security and stability of cyberspace, as well as the importance of an inclusive approach.

In our submission, we follow the template and style guidance provided for the RFC, in order provide comments and additional feedback on the six proposed norms and their accompanying background notes. We also suggest a new norm on inclusive cyber policy processes.

Feedback on Section 1: “Explanation of the Norm Package and Focus of the GCSC”

We also take this opportunity to provide feedback on section 1 of the Norm Package Singapore, the “Explanation of the Norm Package and Focus of the GCSC”. We suggest a rewording of the following sentence: “Throughout its deliberations, the GCSC is guided by significant shared core beliefs. These include (…) the need to balance rights and responsibilities for both states and individuals.”

We do not believe that this wording accurately reflects the obligations and responsibilities that stem from international human rights law. Rights and responsibilities are not to be balanced; rather, human rights must be respected and protected with any restrictions only permitted where these would be consistent with the state’s obligations under international human rights law and the equivalent responsibilities of private enterprises under the United Nations Guiding Principles on Business and Human Rights. We suggest the following rewording of the sentence identified above which we believe would also assist in the interpretation of the norms beyond the background notes by framing them in a manner consistent with state’s obligations and private enterprises’ responsibilities under international human rights law:

“The GCSC is also mindful of the strong links between cybersecurity and human rights and that measures taken to ensure the stability of cyberspace can both strengthen the protection of human rights, but also pose risks to them. As such, the GCSC has also been guided by its firm belief in the importance of ensuring that all measures taken to implement these norms are consistent with states’ obligations and the private sector’s responsibilities (under the UN Guiding Principles on Business and Human Rights) under international human rights law. This includes, for example, ensuring any measures which potentially restrict human rights have a clear legal basis, are in pursuance of a legitimate aim, and are necessary and proportionate.”

1. NORM TO AVOID TAMPERING

Introduction

We understand that the norm to avoid tampering is designed to promote and protect the stability of cyberspace by ensuring that vulnerabilities are not intentionally introduced into digital technologies and systems. However, the current wording of the norm and the background note could support tampering in ways that would impair the stability and security of cyberspace. Our suggested changes to the wording of the norm and the accompanying background note are designed to safeguard against potential misinterpretation of the norm and to ensure that there is consistency between the norm and the background note.

Norm

Recommended rewording

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

Rationale

Products which are either being developed or are in production should never be tampered with, as tampering often occurs with the intention of introducing new vulnerabilities (as opposed to exploiting vulnerabilities that already exist post-development or production, often as a result of unintentional programming or product development errors). In its original form, the norm risks legitimising the creation of vulnerabilities which should be contrary to the intent of the norms and purpose of the GCSC.

Background

We recommend rewording the background note where it says "targeted interception and tampering of a limited number of end-user devices in order to facilitate military espionage or criminal investigations" to "Any state tampering of end-user devices should be subject to legal requirements and processes which are underpinned and respect international human rights law and standards, including the principles of legality, necessity and proportionality". Therefore, the entire paragraph could be reworded as follows "it is important to note that the norm prohibits tampering a product or service line, which puts the stability of cyberspace at risk. Any state tampering of end-user devices should be subject to legal requirements and processes which are underpinned and respect international human rights law and standards, including the principles of legality, necessity and proportionality".

The background note states "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". However, this does not refer to tampering during production or development, but rather after production and development. It is also unclear how "little risk to the overall stability of cyberspace" is defined or what determination would be used to determine the legality of the aims outlined, e.g "to facilitate military espionage or criminal investigations". Therefore, there is a discrepancy between the norm and the background note. The current wording provides for a wide margin of interpretation, and potential abuse, of the option of state actors' tampering with devices (also sometime referred to as 'government hacking' or 'state hacking').

As such, there is a need to strengthen the wording in order to guard against potential misinterpretation and to introduce safeguards, due to the security risks entailed by tampering with devices.

Implementation

The norm "state and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with" can be implemented at the national level through inclusion in national cybersecurity strategies of support for strong encryption and other technologies that protect against unauthorised access to systems and devices. Further, states should not introduce legislation that legitimises tampering with devices during development or production. They should not amend existing interception legislation or create new legislation which permits the tampering of end-user devices except in clearly circumscribed circumstances, and subject to judicial oversight.

Supporting documents

- Norm three of the "Report of United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security (2015)", which reads "states should take steps to ensure supply chain security, and should seek to prevent the proliferation of malicious ICT and the use of harmful hidden functions" (see here)
- Microsoft Tech Accord (see here)

Examples

In terms of tampering with devices during development and production, often referred to as the insertion of 'backdoors' in software and hardware, there is little transparency around these practices and allegations of state-engineered or sanction insertion of backdoors into software or hardware are often refuted or difficult to validate (see here and here).

In terms of tampering with devices post-production, referred to as "tampering with end-user devices" in the background note, this practice is increasing, although it is often opaque and difficult to trace. Some states use legal avenues, often through the use of existing interception legislation (see here) or creation of new legislation which provides state agencies with the power to tamper, or hack devices (see here). However, as noted above, tampering with devices post-production poses serious risks to the stability and security of cyberspace.

2. NORM AGAINST COMMANDEERING OF ICT DEVICES INTO BOTNETS

Introduction

We consider the norm against commandeering of ICT devices into botnets to be an important one, and we don't suggest any changes to the norm itself. However, we suggest changes to the background note, in order to provide clarification and to guard against misinterpretation of the norm which could risk increased growth in the use of botnets, and pose threats to the security and stability of cyberspace.

Norm

We do not suggest any changes to the norm itself.

Background

We suggest removing the text "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." This wording risks encouraging the hoarding of vulnerabilities for state or state surrogate (non-state) use. Secondly there is a lack of clarity with regards to definitions of "individual adversary" and "group of adversaries" as it is unclear whether state or non-state actors are being referred to.

Therefore we suggest removing this text and replacing it with "The use of botnets by state actors, or by non-state proxies of state actors, poses a threat to the stability and security of cyberspace. States should develop defensive capabilities, including risk management practices, to protect infrastructure from DDoS and botnet attacks. As combatting the growth and use of botnets requires cooperation with other stakeholders including ISPs, industry and end-users, they should promote the principle of shared responsibility in cybersecurity by engaging in cross-stakeholder dialogue and cross-border cooperation. High-level and intelligent information sharing that prioritises the sharing of relevant and required information which respects user rights, in particular with regards to privacy and data protection, is required to address the threat and use of botnets."

Implementation

This norm can be implemented by:

- Promoting industry legislation and standards to prevent and mitigate botnets that promote user safety and protect user rights
- Supporting the work of researchers, including on the prevention and handling of botnets
- Engaging in multistakeholder and cross-border cooperation efforts which promote transparency and relevant information-sharing for mitigation of botnets and for the enforcement of the legal and technical measures that address the creation, propagation, and functioning of botnets

Supporting documents

- ENISA (2011) "Botnets: Detection, Measurement, Disinfection & Defence" (see here)
- OECD (2012) "Proactive Policy Measures by Internet Service Providers against Botnets" (see here)

Examples

No examples provided

3. NORM FOR STATES TO CREATE A VULNERABILITY EQUITIES PROCESS

Introduction

The exploitation of software or hardware vulnerabilities is one of the main risks to the security and stability of cyberspace. As such, any hoarding of vulnerabilities can contribute to the instability of cyberspace. Our suggested rewording is intended to acknowledge the security risks posed by the storing and use of vulnerabilities.

Norm

Recommended rewording

Remove "whether" and reword the norm so it reads "States should create procedurally transparent frameworks to determine 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."

Rationale

No vulnerabilities should ever be indefinitely retained as retention of vulnerabilities poses risks to the stability and security of cyberspace. Instead, part of setting up a vulnerabilities equities process (VEP) will be to identify the appropriate stage at which a given vulnerability should be disclosed, with consideration to a range of perspectives. The suggested new wording both clarifies and emphasises this important aspect of a VEP.

Background

We suggest rewording the reference to the use of vulnerabilities to reflect their very damaging effect on the stability and security of cyberspace and therefore the need to circumscribe their use to very limited circumstances.

Therefore, we suggest rewording "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" to "a key part of this is the creation, by states, of a process for disclosure that takes into account the full range of policy, economic, social and technical equities" because, as noted above, no vulnerabilities should ever be indefinitely retained.

The text currently states "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." This statement conflates the various uses of vulnerabilities by different actors for the purposes of tampering or 'hacking' - including military and law enforcement uses. Further, the evidence base for this statement has not been made clear, and there are a variety of tools, including training for law enforcement agencies on accessing evidence in the cloud that can support the needs of law enforcement agencies in the digital age and present far fewer security risks to the stability of cyberspace than the use of vulnerabilities.

Therefore we would suggest removing "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" and rewording the paragraph so it reads "States often argue that they must preserve at least some select capabilities, including the use of undisclosed vulnerabilities in order to use in intelligence and criminal investigations. This use of vulnerabilities must be limited, subject to transparency requirements such as legislative oversight and other legal safeguards, all of which should be clearly outlined in a VEP."

We would also suggest adding references to the following important elements of a VEP, outlined below:

- A reference to the need to protect the rights of security researchers, in order to incentivise them to disclose vulnerabilities in a responsible manner. Researchers can be disincentivised from disclosing vulnerabilities due to legal uncertainty, and fear of being exposed to civil or even criminal liability for their work.
- A reference to a need to ensure inclusivity in the process of developing and implementing the VEP including engagement with civil society, private sector, academia and other experts as relevant.
- Non-disclosure agreements with third parties/other contractors should be prohibited or very limited as these detract from the transparency of a VEP.

Implementation

Stakeholders can move towards implementation of this norm by instituting a VEP development process, through an interagency coordinating mechanism such as a Secretariat. They should also study VEPs in other states and coordinate accordingly in order to ensure consistency and coherency between VEP regimes. In order to be subject to maximum transparency, scrutiny and compliance VEPs should be codified in law. Examples of VEPs are included in the literature referred to below.

Supporting documents

- The Centre for European Policy Studies (CEPS) "Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges" (see here)
- Stiftung Neue Verantwortung "Governmental Vulnerability Assessment and Management" (see here)

Examples

No examples provided

4. NORM TO REDUCE AND MITIGATE SIGNIFICANT VULNERABILITIES

Introduction

Reducing or mitigating vulnerabilities is key to the stability and security of cyberspace. Our suggested changes focus on the importance of setting up coordinated mechanisms for reducing and mitigating vulnerabilities, due to the complex and distributed nature of the digital technology supply chain.

Norm

Recommended rewording

We suggest changing "should prioritize security and stability" to "should prioritize security and resilience by employing 'security by design' principles". In addition, we suggest changing "all actors have a duty to share information on vulnerabilities" to "all actors have a duty to share information and coordinate on vulnerabilities".

Rationale

The term "resilience" is a more relevant concept in relation to the development of products and services than "stability" and 'security by design' principles relate to the full cycle of product development, and also refer to an established software engineering set of principles.

The inclusion of the reference to coordination encompasses a greater variety of activities and actors which are important for vulnerability disclosure from sharing information to patching of vulnerabilities.

Background

We suggest including reference to the development of robust and transparent coordinated vulnerability disclosure (CVD), in order to ensure consistency with the suggested change of wording to the norms. CVDs can be defined as "a form of cooperation in which a reporter informs a manufacturer or owner of the information system of a vulnerability, allowing the organisation the opportunity to diagnose and remedy the vulnerability before detailed vulnerability information is disclosed to third parties and/or the general public" (Global Forum on Cyber Expertise).

Establishing a coordinated vulnerability disclosure (CVD) policy should be seen as an important priority for any state. They should also be seen as an important part of any developer, manufacturer or vendor of digital technologies security policies, particularly due to the highly distributed nature of the ICT/digital technology supply chain where reducing or mitigating vulnerabilities requires the cooperation of a range of actors.

Implementation

This norm can be implemented in the following ways:

- States can institute a national CVD policy or incorporate CVD into a national cybersecurity strategy
- States can institute regulatory requirements for product safety design
- States can support CVDs by promoting voluntary cybersecurity certification schemes, which can include the establishment of an institutional CVD as a requirement for certification
- States can promote and foster awareness of good CVD practices
- CERTs or CSIRTS as well as private sector companies can institute CVDs and coordinate through voluntary mechanisms or agreements (see Microsoft and GSMA)

Supporting documents

- Paris Call for Trust and Security in Cyberspace (see here)
- United Nations Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security 2013 and 2015 (see here and here)
- Microsoft Tech Accord (see here)
- OSCE Confidence Building Measures to Reduce the Risk of Conflict Stemming from the Use of Information and Communication Technologies (see here)

Examples

No examples provided

5. NORM ON BASIC CYBER HYGIENE AS FOUNDATIONAL DEFENSE

Introduction

We do not suggest any changes to the norm or to the background note.

Norm

We do not suggest any changes to the norm.

Background

We do not suggest any changes to the background note

Implementation

This norm can be implemented at the national level through:

- Legislation which requires or encourages steps to be taken by public and private sector organisations, as well as individuals, to improve cyber hygiene, such as the proposed Promoting Good Cyber Hygiene Act in the USA.
- Establishment of minimal security requirements for industry actors and government agencies (these can also be outlined in legislation)
- Certification or accreditation mechanisms for companies to promote compliance with security standards
- Development and implementation of cybersecurity strategies which incorporate reference to minimal cyber hygiene standards required of industry, as well as monitoring processes for ensuring compliance

Supporting documents

- Promoting Good Cyber Hygiene Act in the USA (see here)

- ENISA (2017) “Review of Cyber Hygiene Practices” (see here)

Examples

No examples provided

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

Introduction

We do not suggest any changes to the norm itself. Our suggested comments relate to the background note and suggest clarification on some of the points made therein, particularly with regards to the use of offensive cyber operations.

Norm

We do not suggest any changes to the norm itself.

Background note

Recommended rewording

We suggest removing “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” and replacing with “Offensive cyber operations can be damaging to the stability and security of cyberspace and states should therefore take coordinated steps to limit the proliferation of cyber offensive measures by all actors”.

Rationale

The suggested rewording supports the reduction of proliferation of cyber offensive measures and guards against the risk of escalation in use of cyber offensive measures by all actors. It also takes into account the relationship between non-state and state actors in conducting offensive cyber operations whereby non-state actors are often used as proxies by state actors. The rewording promotes the view that it is ultimately the responsibility and aim of states to collectively reduce the proliferation of offensive cyber operations.

Implementation

This norm can be implemented in the following ways:

- States should develop and implement, in an open, inclusive and transparent manner, a vulnerability equities process as well as develop and support coordinated vulnerability disclosure processes (see “Norm to Reduce and Mitigate Significant Vulnerabilities” and “Norm for States to Create a Vulnerability Equities Process” above)
- States should not stockpile zero-day vulnerabilities
- States should take steps to implement the 11 voluntary non-binding norms included in the UN GGE 2015 report (A/70/174)
- States should cooperate and invest in confidence building measures

Supporting documents

- Microsoft Tech Accord (see here)
- UN GGE Reports 2013 and 2015 (see here and here)

Examples

No examples provided

NEW: Norm on inclusive cyber policy processes

Norm

States should ensure that the development and implementation of cyber-related policies are open, inclusive and transparent. The stability and security of cyberspace both affects and relies on a wide range of stakeholders, and as such requires their meaningful engagement to be effective and sustainable.

Background note

The security and stability of cyberspace relies on the cooperation of a wide range of stakeholders. In addition, measures or actions which impair the security and stability of cyberspace directly impact the rights and freedoms of individuals, and can cause damage to the digital economy.

Implementation

This norm can be implemented by instituting processes which adhere to the principles of multistakeholder development referred to in the supporting documents below. In addition, states can implement the multistakeholder approach by following the guidelines and recommendations for multistakeholder approaches outlined in Global Partners Digital's "Framework for Multistakeholder Cyber Policy Development" (see here) which outlines the approach and relevant characteristics and the report "Multistakeholder Approaches to National Cybersecurity Strategy Development" (see here) which focuses on examples of applying the approach to national cybersecurity strategy development and captures good practice from different countries.

Supporting documents

- UNGA resolution 57/239 on the Creation of Global Culture of Cybersecurity (see here)
- UN GGE Reports 2013 and 2015 (see here and here)
- 2015 Global Conference on CyberSpace Chair Statement (see here)
- Paris Call for Trust and Security in Cyberspace (see here)
- UK-India cyber agreement (see here)

Examples

N/A