Submission from

Kristen Nyman
Fellow, National Security and Cybersecurity
R Street Institute

Kathryn Waldron
Fellow, National Security and Cybersecurity
R Street Institute

Anthony Marcum
Fellow, Governance
R Street Institute

for the

United Nations Open-Ended Working Group
Intersessional Consultative Meeting

on

2-4 December 2019

at the

United Nations Headquarters
New York, NY

on the topic of

Developments in the field of information and telecommunications
in the context of international security

Executive Summary

We at the R Street Institute believe, as many States have asserted, that existing international law applies in the context of information and communication technology (ICT), including the UN Charter in its entirety. As such, we believe that norms related to ICT policy exist, and therefore, going forward, the most valuable action would be to address the finer points of carrying out those norms in a way that balances the need to achieve international peace and security with respect for each country's sovereignty and domestic legal regimes.

In an effort to offer a practical working paper, we have focused our policy recommendations on the proposed questions for consideration and the implementation of various iterations of the Group of Governmental Experts' (GGE) norms. We will address three areas specifically: global supply chain integrity, data localization and cross-border data transfers, and the appropriate global legal framework for implementing cyber norms.

We have included policy language that Members are welcome to incorporate into the 2019-20 OEWG working paper.

OEWG Report Should Focus on Implementation

In 2018, the United Nations General Assembly adopted Resolution 73/27, which established an open-ended working group (OEWG) on developments in the field of information and telecommunications in the context of international security.

As part of the OEWG's work, an informal intersessional consultative meeting with non-governmental organizations (NGOs) and other interested stakeholders is set to begin on 2 December 2019 in New York City. Among the important topics to be discussed are the cyber threat landscape; cyberspace rules, laws and norms; and confidence-building measures between States and non-State stakeholders.

The R Street Institute is pleased to take part in this meeting. Importantly, these discussions will build upon a bedrock of consensus that has developed through the past work of the GGE and Member States. Past GGE reports have already reached consensus on a variety of important matters. The 2013 GGE report, for example, confirmed that international law, "and in particular the United Nations Charter," applies in cyberspace. The 2015 GGE report reaffirmed that international law applies to the use of ICTs by States.

Beyond international law, the 2015 GGE report also included a set of non-binding norms for responsible State behavior. These eleven norms "reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States." These norms are broad but include core State responsibilities such as "not knowingly allow[ing] their territory to be used for internationally

wrongful acts using ICTs," "tak[ing] reasonable steps to ensure the integrity of the supply chain" and "encourag[ing] responsible reporting of ICT vulnerabilities."

Despite these core agreements, there remain several significant divergences between States. Although past GGE reports have reaffirmed that international law applies to cyberspace, stakeholders disagree on the applicability of international humanitarian law (IHL). There is also disagreement about whether to create a new cyber convention.

These debates are complex, and stakeholders have raised numerous arguments concerning these topics. Indeed, the 2017 GGE largely failed to reach a consensus on the applicability of international law to the use of ICTs by States. But although difficult questions remain, so much past progress toward identifying cyber norms and principles should not be negated by marginal disagreement. The 2020 OEWG report would best be served by focusing on the implementation of norms already developed through international consensus.

To that end, this paper addresses three subjects that we believe will assist with the implementation of largely agreed-upon norms and shed light on some of the more complex legal and technical issues of global data security. We believe this guidance will serve the UN's purpose and its mission on this subject to create a secure and peaceful ICT environment.

Integrity and Security of the Global Supply Chain

ICTs are already deeply embedded in the average person's daily life, and the development of 5G and other future technologies will only increase the pervasiveness of ICTs. As ICT's ubiquity grows, so too does the need to protect the integrity of the ICT supply chain. The complexity of the modern ICT supply chain can lead to a worrying opacity, as governments, companies and even private individuals struggle to identify potential threats. Concern about poor cybersecurity—or worse, backdoors or other systematic vulnerabilities mandated by foreign governments—are becoming commonplace. Consider the furor over companies like Huawei in the United States. If not addressed, these fears have the potential to damage economic relations, threaten States' national securities and undermine global trust.

The Member States of the UN's GGE have already acknowledged the vitality of protecting the ICT supply chain. The 2013 GGE report acknowledges supply chains' critical role, saying, "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services."[1] The 2015 GGE report goes a step further and includes supply chain integrity as one of the voluntary norms, stating, "States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of

[1] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 68th United Nations General Assembly, June 24, 2013. https://undocs.org/A/68/98.

harmful hidden functions."[2] While the inclusion of this norm is an excellent next step, the 2015 GGE report did not offer further explanation on what types of actions count as "reasonable steps."

The 2020 OEWG report has the opportunity to determine what these "reasonable steps" will be. In considering which practical steps best implement the spirit of the 2015 GGE norm, it is important for States to bear in mind that supply chain integrity isn't just about employing specific technical solutions, although technical solutions can and should play an important role in any State's ICT strategy. Supply chain integrity is about global trust. It's not enough for States to talk about the importance of supply chain integrity in the context of international convenings. They must also implement domestic policies that refrain from excessive government manipulation of and/or intervention in the ICT supply chain.

Therefore, we propose the following implementation strategies of previously agreed-upon norms that any Member States may adopt:

1. States should agree not to force ICT companies to include backdoors in ICT devices and avoid other systematic government interventions in the ICT supply chain. States should also publicly condemn any government-sponsored or -approved activities that intentionally violate supply chain integrity.
2. States should pass domestic laws and international treaties that make it easier for companies to reveal discovered vulnerabilities and share information about potential risks.
3. States should promote risk management practices among industry stakeholders within their own borders.
4. States should agree to promote market competition of ICT companies and not impose undue market barriers.

Building backdoors into ICT devices or mandating access to ICT data through "golden keys" can seem alternately appealing and alarming when it comes to a State's national security. The idea can be appealing because of the wealth of information ICT data could potentially provide a government regarding the activities and communications of criminals and potential terrorists. But the idea is equally alarming because non-domestic companies may be forced to provide data on a State's citizens to a foreign government, and rogue States can use data to persecute protesters or political opponents. Our scholars acknowledge that allowing encryption without backdoors comes with social costs for law enforcement and other agencies, and that States have the right to maintain sovereignty over their own borders. However, we believe the risks of backdoors and "golden keys" outweigh the benefits.

---

[2] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 70th United Nations General Assembly, July 22, 2015. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

Our second proposed implementation strategy stems from the difficulty of assessing which links in the supply chain present unacceptable risks. The risk of a specific supplier may come from a variety of different sources, including the supplier's history and structure (e.g., previous instances of cyber espionage and/or close ties with hostile foreign entities) and the history and legal structure of the supplier's home country (i.e., the likelihood said supplier could be forced by a hostile foreign government to allow access to private data). However, industry stakeholders may not have access to such information for a variety of reasons: Companies may not want to reveal information about previous breaches for fear of exposing their own security vulnerabilities or to protect their reputation with consumers. Important information could be considered classified by government agencies and therefore hidden from the private sector. To identify potential supply chain risks more easily, States should consider how they can break down these information barriers. They should look for opportunities to build private-public partnerships, like public commissions to assess the security of existing ICT supply chains and publish results.

Similarly, our third proposed implementation strategy will require States to work in close connection with industry stakeholders. States cannot bear all the responsibility for supply chain integrity. Members of the ICT industry, being on the front lines of a barrage of malicious cyber activity, must proactively install rigorous cybersecurity controls. States should seek ways to encourage this, such as making sure than existing ICT regulations do not provide perverse incentives in regards to assigning responsibility for cybersecurity breaches.

Our final suggested norm implementation strategy may seem like a non sequitur, given the topic at hand. A State worried about the security of its own ICT systems may consider favoring one domestic supplier as an attempt to protect its national security. But such strategies are counterproductive. Market competition can promote cybersecurity as companies seek to make their products more secure than the competition's. Our R Street colleague Charles Duan succinctly describes this phenomenon:

> Computer security is a value-added benefit to consumers, so firms in competitive markets are likely to use security improvements to gain an edge over their competitors, and are likely to poke holes in their competitors' products to draw consumers away from them. By contrast, monopolized markets offer less external impetus to test products for flaws, and a monopolist may choose to focus less on security and more on new product features or increased product quality.[3]

Supply chain integrity can be damaged just as easily by lax security standards and monopoly market control—where one vulnerability may be enough to bring down entire systems—as by

---

[3] Testimony of Charles Duan, Senate Committee on the Judiciary, "5G: National Security Concerns, Intellectual Property Issues, and the Impact on Competition and Innovation," 116th Congress, May 14, 2019. https://www.rstreet.org/2019/05/23/5g-national-security-concerns-intellectual-property-issues-and-the-impact-on-competition-and-innovation-submitted-statement-of-charles-duan/.

malicious activities by rogue states. But regardless of an attack's source, diversification in the marketplace can protect against a systematic collapse or crisis.

The global consequences of any government systematically undermining the integrity of ICT supply chains would extend far beyond economic loss. Violating supply chain integrity would directly diminish international trust, making our world far less secure. R Street urges stakeholders to approach supply chain security with a long-term perspective that maintains international peace and security.

Data Localization and Cross-Border Data Transfers

With an increasingly interconnected ICT global community comes a massive volume of valuable data on human activity. As a result, companies want to move data freely across borders to facilitate economic and social activity, while governments want to protect it for their purposes. This brings us to a finer point of the global data regulation debate, one on which we believe it is possible to achieve a majority consensus: data localization and cross-border data transfers. Regardless of the desires of various equities involved in this discussion about fluidity of and access to data, one principle remains true: Internet commerce and communication thrive on the free flow of information and open sharing of data. Digital borders will only harm the global economy, breed mistrust among various equities and induce insecurity in an already insecure cyber environment.

Increasingly, States have begun to implement data localization laws that require all data generated within the country to be physically stored there. These blanket data localization practices are simply a second iteration of Internet border controls, the first being censorship. The international community has condemned unjustified restrictions on the flow of information into a country—i.e., censorship. It must now condemn unjustified restrictions on the flow of information out of the country—i.e., data localization.

We understand the desire for Member States to keep the value of their data within their borders to avoid intellectual property theft, restrict foreign suppliers from infiltrating delicate domestic markets or readily access useful information. However, these rationales do not comport with the purpose of the UN—above all, to maintain peace and security.

The OEWG must recognize that there are illegitimate purposes for restricting the free flow of data. Economic protectionism is one such illegitimate reason. We fear that States may express legitimate reasons for localizing data as pretenses for illegitimate purposes, and we therefore implore Member States to define what they consider legitimate and strongly condemn actions outside of that issued guidance.

As for legitimate purposes, we would encourage Member States to consider that data is not safe solely because it is stored within their own borders. If a government is concerned with what we would call a justified event (e.g., law enforcement access to data relevant to a cyber incident or

the general mishandling of private personal data), then we would encourage member states to consider, when appropriate, retaining supervisory access over such sensitive data and requiring copies to be stored domestically without restricting cross-border data transfers altogether.

And while these policies remain our recommendations for best practices, we recognize and affirm each Member State's right to sovereignty and concede that not every Member State will agree to such limited data localization practices. Therefore, for states who are unable or unwilling to abide by this global norm, we would recommend that bilateral or multilateral treaties be utilized to achieve clarification on cross-border data transfer regulations. In the instance of law enforcement activity, for example, we recommend the use of mutual legal assistance treaties (MLATs) to ensure that, for instance, in the event of a cyber incident, a data subject's home state may access the relevant information if deemed necessary and appropriate. With company-to-data subject agreements, we would recommend utilizing contract clauses, presented in plain language, to ensure that consumers have access to information about what their data is being used for and have recourse with the host state in the event of a cyber incident, misuse or mishandling of data.

Of course, even these treaties may not be enough to ensure that each country is willing to lift data localization restrictions to the degree necessary to facilitate free and open data sharing practices. In an instance where such an agreement cannot be met, such as companies refusing to allow host States to retain data from another home country's data subjects, we recommend that encryption and other cypher technology be utilized to secure the data but still abide by the country's localization laws. During a justified event, and if an agreement between all equities is garnered, the government could request an encryption key from the company in the data subject's home country. (We would urge clear guidance on the ability of governments to demand encryption keys by way of bilateral agreements.) As a rule, and in accordance with existing international law, we would argue that the States who should create agreements to request access to such information during a justified event would be the data subject's home country, the host country in which the incident took place and, if relevant, the ICT company's host country. Again, we implore member states to utilize multilateral agreements to facilitate transparent and efficient data sharing and cross-border investigation practices.

As we discuss facilitating data transfers, it is important to acknowledge that not all data recipients will be equipped with the cybersecurity and privacy standards that are necessary to secure data adequately. In these cases, we look to the European Union's General Data Protection Regulation (GDPR) Articles 45-49 for guidance and recommend a version of it be adopted globally, with some modifications.[4] We highly recommend that any cross-border data sharing arrangements adhere to two main principles: the availability of enforceable data subject rights and effective legal remedies for data subjects.

---

[4] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

Data is valuable and must be protected. However, there are remedies that do not unduly restrict the free and peaceful flow of data across borders. Erecting digital borders will only weaken the global economy, and we strongly urge each Member State to consider this proposal as an alternative to data localization and restrictive data access laws.

Legal Framework to Address Malicious Cyber Actions

Although the 2020 OEWG report should focus on implementation—including the policy topics addressed above—it is also important to look forward and consider the ongoing debate on how international law applies in cyberspace.

For example, it is debatable whether a new legally binding agreement is necessary to address global cybersecurity challenges. Indeed, both private industry and Member States have made proposals for a new convention. A future convention may ultimately be useful. After all, a comprehensive cyber convention could serve as an important source of international law and provide greater legal clarity for Member States. Nevertheless, Member States and stakeholders must first prioritize the domestic implementation of norms before turning to longer-term international agreements. The unique and evolving challenges of the ICT environment suggest this approach.

Of course, a new cyber convention would not be the first of its kind. The Convention on Cybercrime of the Council of Europe (Budapest Convention), for instance, has been signed and ratified by dozens of States.[5] The Budapest Convention—the only modern agreement of its kind—has been a success, but as technology evolves, the agreement has required consistent upkeep. To address these changes, negotiations for a Second Additional Protocol to the nearly twenty-year-old Budapest Convention are currently underway. A similar fate would likely befall any new cyber convention, despite its positive merits.

Even if the process began for a new cyber convention, it should not distract from the implementation of previously agreed-upon cyber norms. After all, through negotiation and consistent developments in ICTs, a new cyber convention has the potential to be both over- and under-inclusive. It could instill legally binding restrictions that could unintentionally limit ICT advancement and fail to address every category of agreed-upon norms, resulting in the unfortunate prioritization of some norms over others.

Further, the strength of many conventions—like the Budapest Convention—is their ability to serve as guides for Member States to craft domestic legislation and policies that are more

[5] "Chart of signatures and ratifications of Treaty 185," The Council of Europe, Status as of Dec. 2, 2019. Retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Ep4KjKYI.

uniform and helpful across the globe. The implementation of norms asserted in the 2015 GGE report already serves this purpose.[6]

This implementation can in part be guided by current international law. The 2015 GGE report repeated that "[t]he adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in" cyberspace. Additionally, one of the norms included in the same report stated that States "should not conduct or knowingly support ICT activity contrary to its obligations under international law …."[7]

Nevertheless, it is disputed whether certain aspects of international law, including international humanitarian law (IHL), apply in cyberspace. We believe IHL does apply and are not persuaded that IHL would invite greater conflict and eager military retaliation for cyber mischief. Many of these fears, for example, fail to consider IHL's principles of necessity, humanity, distinction and proportionality.

Another area for consideration is a legal framework for dealing with "intellectual property theft," which has been a growing topic of conversation in recent years. Caution is advised in developing these frameworks because of the indeterminate phrase "intellectual property," which can potentially oversimplify many different types of information and legal regimes. The malicious actions generally referenced under the "IP theft" umbrella are corporate espionage and government-mandated disclosure of company-confidential information; both, thus, deal with the type of IP known as "trade secrets," which derive value from not being made public. Yet IP also covers patents, copyrights, trademarks, rights of publicity, and other such legal exclusivities and protections that are not amenable to "theft." One need not steal an invention from a published patent, for example, since the text of the patent is freely available to the public. Altering patent protection, then, would have no real effect on either of the problems generally characterized as "IP theft." It is thus advisable to be specific about the type of intellectual property in question and ensure that legal frameworks and measures are correctly tailored to the harms at issue.

These debates, however, can remain separate from the ultimate OEWG report, which should prioritize the pragmatic implementation of existing, agreed-upon norms.

Concluding Remarks

We thank the United Nations for hosting this important and timely discussion. We hope that our contributions helpfully inform the evolving conversation on security of the global cyber network. If any stakeholder or Member State has questions or comments, please do not hesitate to reach out to our team at the R Street Institute.

Respectfully,

---

[6] "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," 70th United Nations General Assembly, July 22, 2015. https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[7] Ibid.

Kristen Nyman
Fellow, National Security and Cybersecurity
knyman@rstreet.org

Anthony Marcum
Fellow, Governance
amarcum@rstreet.org

Kathryn Waldron
Fellow, National Security and Cybersecurity
kwaldron@rstreet.org