Advancing International Cyber Norms:

Multistakeholder Recommendations

Introduction from the Co-Chairs

Cyberspace continues to provide unparalleled opportunities for innovation, development and prosperity. However, at the same time threats emanating from cyberspace continue to grow, as does the realization among governments, industry and civil society that no single stakeholder group can effectively tackle these challenges alone.

Instead, a multistakeholder approach is needed.

The Paris Call for Trust and Security in Cyberspace (the Paris Call) provides a platform for just such an approach. The Paris Call is today endorsed by about 80 states, 35 public authorities and local governments, more than 700 companies and almost 400 civil society entities – more than 1200 supporters in total. This represents the largest group ever assembled in support of a cybersecurity focused agreement, a truly unprecedented action in the realm of international security and stability online.

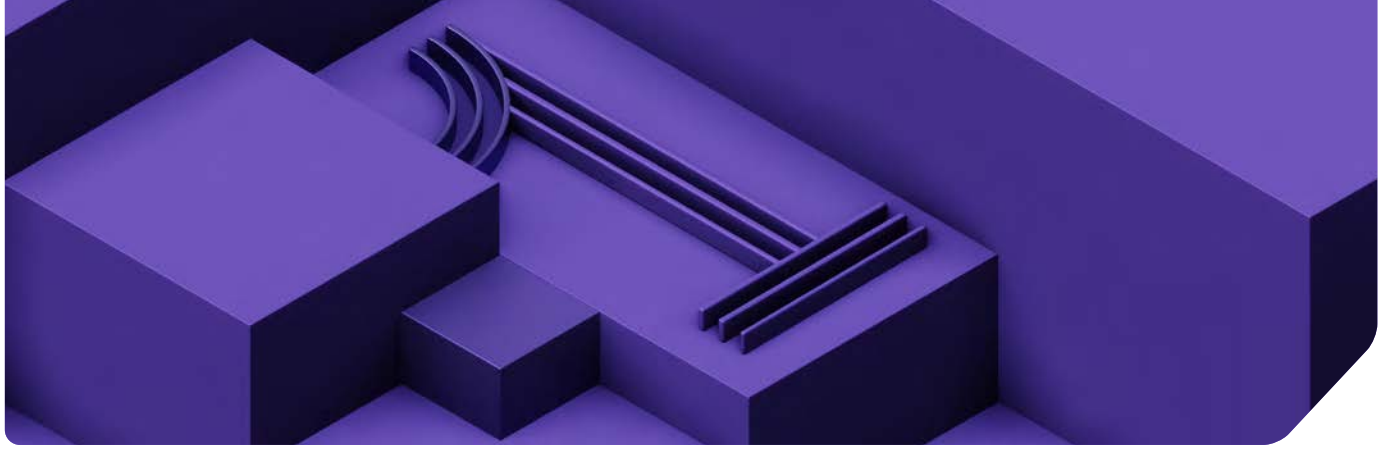
However, not only have more groups joined the Paris Call since its inception in 2018, its significance has grown as a result of the work by signatories to implement the nine Paris Call principles. Along the way they have created a genuine Paris Call Community – a community focused on delivering tangible outcomes within the framework of the Paris Call.

The six Paris Call Working Groups, launched at the 2020 Paris Peace Forum are the latest expression of this ambition. The different working groups sought to tackle challenges identified as part of the drafting of the Paris Call, as well as to help clarify the different principles and enable the supporters to implement them. Microsoft, F-Secure and the University of Florence were proud to have joined together to co-chair Paris Call Working Group #4 on Advancing International Cyber Norms. Throughout 2021, we organized several multistakeholder workshops, each addressing the cyber norms landscape and its relation to the nine Paris Call principles. During these workshops, key observations, ideas and lessons learned were collected from a diverse group of experts, practitioners and stakeholders. Based on what we heard and learned in these discussions, we have distilled a compendium of multistakeholder recommendations that we hope will be valuable to practitioners across all stakeholder groups going forward.

Perhaps the message that we heard the loudest was a call for more systematic and meaningful multistakeholder discussion and co-operation of these issues – yet another stark reminder that not only do all stakeholders need to do *more*, but that they need to do more *together*.

Contents

The contents of this Compendium are based on the insights, ideas and discussions heard at a series of Working Group meetings held throughout the year. As such, they reflect the diverse perspectives and expertise of a truly multi-stakeholder group, not necessarily the views of individual participants, the Co-Chairs or the French Ministry for Europe and Foreign Affairs.



Paris Call Principle #1

Protect individuals and infrastructure

In addressing this issue in its very first principle, the Paris Call for Trust and Security in Cyberspace recognized the importance of preventing and recovering from malicious online activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure. This is all the more crucial, given that threats emanating from cyberspace continue to increase.

Given that this trend is not in the interest of any stakeholder group – be they governments, industry, civil society or individual users – it is crucial to continue discussions in terms of what can reasonably be done to better protect individuals and infrastructure.

Clearly, this is a complex challenge. For example, when it comes to critical infrastructure, no universal agreement exists in terms of what exactly constitutes such infrastructure. That said, it is noteworthy that the consensus report of the 2021 United Nations Group of Governmental Experts (UN GGE) provides a degree of much needed clarity to the conversation when it enumerates a non-exhaustive list of specific sectors that should be considered "critical infrastructure" and off-limits to attack. It includes "healthcare and medical infrastructure," which is particularly relevant given the ongoing COVID-19 pandemic as well as "energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes."

Acknowledging the desire by some states to retain strategic ambiguity, it is nonetheless important to continue efforts that provide greater clarity in terms of which infrastructure should be off limits to cyberattacks.

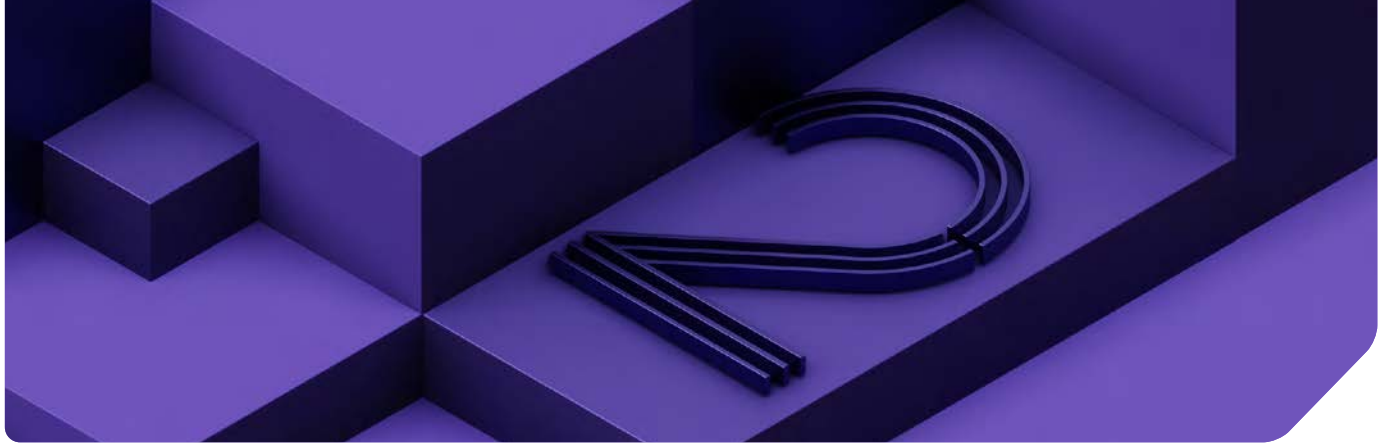
With this in mind, Working Group 4 participants appropriately agreed on the importance of a multistakeholder approach. They acknowledged several significant issues as needing work, including: greater clarity and consensus regarding what norms mean and how they can be implemented; increasing civil society's role in this discussion, which is currently inadequate; engaging law enforcement who often abstain from addressing cybersecurity issues given that these are frequently – inaccurately and unhelpfully – characterized as the sole responsibility of the given institution's information technology (IT) department.

Building on the above, the key recommendations made by Working Group 4 participants when discussing the need to protect individuals and infrastructure are:

- It is essential to **adopt a multistakeholder approach** that involves not just governments but also the private sector, think tanks, academia, and civil society collaborating and coordinating as appropriate.
- As reflected in a survey conducted by KPMG and Microsoft, more work is needed in the areas of **incident response planning** and **supply chain management** (see also report of June 10, 2021 workshop with GMF on supply chain infrastructure).
- As also reflected in the aforementioned survey, norms are currently "**fuzzy**," so **greater clarity and precision** should be provided – and consensus should be fostered – regarding their precise intended meaning. The European Union's (EU) current work on re-writing the Network and Information Security (NIS) directive could be one source of inspiration, as that language is expected to be quite clear and precise.
- Relatedly, entities outside government (e.g., critical infrastructure providers) are often not intrinsically familiar with cybersecurity norms – therefore **spreading awareness widely** on what norms entail and how to implement them remains key.
- To help make cybersecurity norms more accessible, **a useful starting point** could be to **consolidate the "top" norms** into one document. This could involve compiling the norms that currently exist across the various sources, and then sharing that single document with multistakeholder groups to develop consensus regarding what the "top" norms are.
- **Defining critical infrastructure** is vital. The recent GGE and OEWG reports made welcome advances in this regard by enumerating specific examples of critical infrastructure.
- It is important to **distinguish between traditional armed conflict and cyberattacks**. Relatedly, from an international law perspective, cyberattacks often do not qualify as armed attacks, so it is important to consider how norms and rules apply below the threshold of armed conflict.
- Increasing **accountability for non-State actors** will be critical, given that while States can subscribe to norms, that may not be the case with non-State actors. Relatedly, it is important to consider how norms may relate to proxy operations – i.e., where non-State actors act on State actors' behalf.
- **Civil society** should play – and should be encouraged to play – a larger role on this issue. It currently has a limited voice. It is not advocating as actively as it could given bureaucratic hurdles.
- **Law enforcement** should be engaged. Cybersecurity incidents are crimes and law enforcement is responsible for protecting individuals and infrastructure from malicious activity. Referring to cyber incidents only as "cybersecurity" or only as relating to "cyberspace" could discourage the involvement of law enforcement by making it seem that these issues are far beyond law enforcement's capabilities and that they are the responsibility of the given institution's IT department.

Recommended reading & resources shared by participants

- Group of Governmental Experts on Advancing responsible State Behaviour in Cyberspace in the Context of International Security (2021 Final Report): https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf
- Open-ended working group on developments in the field of information and telecommunications in the context of international security (2021 Final Report): https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf
- Combating Ransomware – A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force: https://securityandtechnology.org/wp-content/uploads/2021/09/IST-Ransomware-Task-Force-Report.pdf



Paris Call Principle #2

Protect the Internet

Paris Call principle #2 is about protecting the Internet. The aim is to "Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet."

Protecting the availability and the integrity of the public core of the Internet requires close cooperation between different types of actors, including non-profit organizations such as ICANN (Internet Corporation for Assigned Names and Numbers), civil society, academia and private companies. Often referred to as the "Cornerstone of the Web", the Domain Name System (DNS) serves as the Internet's directory. This protocol translates a domain name into an IP address, based on a database distributed on thousands of machines. If the DNS fails because of data corruption or a denial-of-service attack, websites and emails become inaccessible.

Responding to threats against the core protocols and services of the global Internet requires the involvement and cooperation of the full range of relevant stakeholders. Most of the infrastructure, services, and products underpinning it are privately-owned, or governed and maintained by the civil society.

Whilst the idea of protecting the core Internet functions has a longer history, the notion had only relatively recently become the subject of various norm proposals, most notably by the Global Commission on the Stability of Cyberspace. To further develop these ideas, the Paris Call Working Group 4 focused its discussion on practical considerations, misunderstandings and awareness raising around protecting the Internet.

Building on the above, the key recommendations made by Working Group 4 participants when discussing the need to protect the Internet are:

- It is important to work with **various stakeholders** to help advance this norm, across business, government, and civil society – including technical advocacy groups, technical coordination groups, rights and advocacy groups, States, and corporate partners.
- It is important to advocate for States and other stakeholders should **use the term "public core" rather than the term "infrastructure" (or "critical infrastructure")**. The Open-Ended Working Group uses the term "critical infrastructure" instead of "public core" but the very reason for using "public core" is to sidestep contested issues regarding what constitutes "critical infrastructure", as different countries have different views on that. Relatedly, infrastructure can be nationalized during a crisis. Therefore, the term "infrastructure" can undermine the **multistakeholder model of internet governance**.
    - It is important to stress that the term "public core" will not inhibit states' ability to conduct law enforcement or intelligence collection; as some actors incorrectly believe.
    - Relatedly, **discussions about this norm should not invoke the broader issue of global commons** – that issue is debated elsewhere and is broader than necessary for the purposes of this discussion. In other words, focus should be on advancing the notion that certain aspects of the internet are part of the public core, without suggesting that all cyberspace is a global common.
- Advocacy and educational efforts should recognize that countries need to work with various parts of their own governments to adopt this norm, and that many of those bodies do not fully comprehend this norm. **Awareness raising and capacity building remain crucial**.
- Efforts to advance the **norm should make clear that it does not create new obligations as it relates to the due diligence principle**. Experience has shown that this is a concern particularly when trying to advance the norm in developing countries.

Recommended reading & resources shared by participants

Global Commission on the Stability of Cyberspace:
https://cyberstability.org/report/

The Importance of Capacity Building

Though articulating norms of appropriate state behavior, confidence building measures and agreement on how international law applies in cyberspace are vitally important, those efforts are of limited utility if countries are not aware of them, or if they don't, or can't, implement that framework. Because cyberspace and cyber threats are borderless, cyberstability is not just the province of a few more developed actors, but also requires the active involvement of the developing world.

Not surprisingly, both the Open-Ended Working Group (OEWG) and Group of Governmental Experts (GGE) reports focused on cybersecurity capacity building as foundational to their mandates. Moreover, the GGE report explicitly recognized that cybersecurity capacity building is a multistakeholder pursuit, noting that "involving other stakeholders such as the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behavior of States in their use of ICTs."

Capacity building can take many forms – from helping states build capabilities to detect, respond to, and cooperate in addressing threats, to helping states implement agreed upon norms, to building diplomatic capability so that states can more fully engage in United Nations and other processes. Yet, as important as it is, and despite a growing demand, cyber capacity building is often under-resourced and under-prioritized. Accordingly, it is important for all stakeholders, including those involved in the Paris Call, to not just echo the OEWG and GGE reports' call for more resources and support for capacity building, but to make that a reality.

In addition, it is important to build on existing platforms – like the multi-stakeholder Global Forum on Cyber Expertise – in order to promote better knowledge sharing and achieve more effective coordination of cybersecurity capacity building around the world. Put simply, effective cyber capacity building is a cornerstone of a peaceful and stable cyber future.

Christopher Painter
President, The Global Forum on Cyber Expertise Foundation

Paris Call Principle #3

Defend electoral processes

Since its inception, the Paris Call has inspired significant efforts related to principle #3. This has included workshops, exchanges among practitioners as well as the publication of good practice guides. For example, one of the most prominent initiatives in implementation of principle #3 was the publication of "*Multistakeholder Insights – A Compendium on Countering Election Interference*", co-championed by the Government of Canada, the Alliance for Securing Democracy, and Microsoft.

As the Compendium on Countering Election Interference noted, bringing communities together to tackle threats and identify practical solutions can help to build resilience against hybrid threats. This is particularly important since, in many places, intelligence services and electoral authorities may not be as familiar or in as regular contact with each other as they should reasonably be. Such lack of resilience is a bureaucratic vulnerability, which further illustrates the importance of efforts to break down unnecessary silos, within and between both the public and private sectors. Looking at the big picture, the importance of effective information sharing among all relevant stakeholders cannot be overstated.

In practical terms, when it comes to determining vulnerabilities, it is vital to consider the ecosystem holistically – every part of the electoral cycle is potentially vulnerable to interference and in need of protection. A system is only ever as secure as its weakest link. Moreover, it is also important to recognize that interference may come from both State and non-state actors. Interference may also not necessarily be a singular event; rather, it can be the set of cumulative effects of individual acts that in the aggregate add up to an impactful act of interference, which may include cyber interference and disinformation. As noted in the Compendium, disinformation in the election environment can often be an indicator that wider hybrid threats are at play. As democracies suffer the impact of these effects, it is crucial to develop a shared language – shared by all relevant stakeholders be they individuals, or representatives from governments, industry or civil society – to discuss threats, threat actors, and responses. Lastly, it is important to recognize that this is a dynamic threat environment which means that responses must also keep constantly evolving.

Many of the findings contained in the Compendium on Countering Election Interference were mirrored in discussion among Working Group 4 participants. Building on the above, the key recommendations made by Working Group 4 participants when discussing defending electoral processes are

- **Fundamentally, international cooperation is key**, as one country could learn from the experiences of another. Additionally, it is essential to adopt a multistakeholder approach that involves not just governments but also the private sector, think tanks, academia, and civil society.
- Defending electoral processes **requires**, inter alia,
  - improving multistakeholder information sharing (including, for example, between governments and social media companies);
  - clearly defining foreign interference and distinguishing it from foreign influence; considering the particular challenges of a pandemic environment;
  - countering disinformation and misinformation;
  - protecting election infrastructure; and building citizen resilience.
- It may be helpful to consider election interference as having **three components** – physical, virtual, and psychological – and to map best practices that counter interference to those components.
- **Capacity-building** is key. It should be a focus area for norms. It is inextricably linked to implementation, and countries are looking for practical guidance. All capacity-building should adopt – and naturally lends itself to – a multistakeholder approach.
- Whenever feasible, it is important to try **to package any new norms as articulations of existing norms**. This is because many countries are hostile toward developing and implementing new norms, including democratic countries that worry about undemocratic countries creating norms to strengthen their oppressive regimes. That said, there is a growing realization that it may be necessary to develop **new norms over time**.
- To help feed into norms-related negotiations happening among countries, stakeholders should **actively engage in multistakeholder forums** such as this (Working Group 4). Such engagement helps widely share and discuss good practices – i.e., "get the word out" including among different sets of stakeholders (e.g., it can help the private sector learn the government's priorities and address them).
- Relatedly, it is important to think about how to bring good practices to practitioners; Canada's Digital Citizen initiative is an example. Additionally, **departments within any given government** should work closely together, rather than in silos.

Recommended reading & resources shared by participants

- Multi-Stakeholder Insights: A Compendium on Countering Election Interference: https://www.canada.ca/content/dam/di-id/documents/compendium-eng.pdf
- Online disinformation (Canada.ca): https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html
- The European Centre of Excellence for Countering Hybrid Threats: https://www.hybridcoe.fi/

The Importance of Multistakeholder Action

Over the past six months, I have had the honor and pleasure to participate in advancing the international norms of the Paris Call for Trust and Security in Cyberspace. Our multistakeholder working group #4 discussed each of the principles with the objective to better implement the norms and make them globally accepted. We openly discussed the values of each of the principles with an appreciation that norms encourage responsible state behavior for the common good, carrying international expectations of states while bearing no state responsibilities.

Our world is confronting increasing threats through cyber means. Violations of sovereignty, theft of intellectual property, damage to supply chain integrity, harm to individuals and infrastructure, and hack-back actions by non-state actors are some of the behaviors we must strive to eliminate to enjoy an open, accessible, stable, secure, and peaceful cyberspace.

As a Canadian who provides advice on such matters to governments, I strongly believe in the safeguarding of inherently governmental functions, specifically our democratic electoral processes. While international law protects tampering of votes and the tallies of votes, it remains insufficiently clear regarding influencing the way voters think.

The challenge of electoral interference through (1) disinformation further spread as misinformation by innocent citizens and (2) the exploitation of our respective domestic laws poses a legitimate threat to our electoral processes.

We must collectively raise the awareness of cyber threats impacting our elections and democratic institutions. We must work together to develop policies, best practices, and methods to prevent and counter cyber election interference, to maintain the sanctity of our electoral processes.

We cannot tackle this alone. Our working group's international delegates offered an environment to listen to each other. It was inspiring to see that we came together virtually, while sitting in different parts of the world, for a common goal of promoting and strengthening the international norms of responsible behavior, all focused to bring peace and stability in cyberspace.

Neal Kushwaha
Adviser, IMPENDO Inc. (Canada)

Paris Call Principle #4

Defend intellectual property

Paris Call principle #4 is about defending intellectual property (IP). The aim is to "prevent ICT-enabled theft of intellectual property, including trade secrets and other confidential business information, with the intent of providing competitive advantages to companies or the commercial sector." There are several international initiatives such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (WTO) and the Paris Convention for the Protection of Industrial Property (WIPO), which call for protection of computer programs, compilations of data or other material and protection against unfair competition. The language of this principle is derived from the G20 Antalya Summit 2015 Communique.

In the discussion it was noted that there are two main areas of IP: industrial property and an author's intellectual property. These have different tools and choices available for protecting the intellectual property rights (IPR) e.g., patents. It was further noted that the Antalya communique was issued in relation to states, whereas Principle #4 is more broadly worded. Nonetheless, this issue is also very closely linked to a more general discussion about responsible state behavior.

Grateful if you could make the following tweak: "Looking at the overall trends, the situation is getting worse. There is also a growing realization of the sheer magnitude of the challenge and that it will be difficult if not impossible to eradicate. Instead, focus should arguably be placed on a risk-based approach that endeavors to mitigate and limit the impact of IP theft as well as on measures that make it more difficult to engage in such behavior in the first place.

In addition, looking at the related issues, it is important to be mindful of potential consequences and escalations that may by be triggered by IP theft, especially if it is of significant impact.

Below are the key recommendations made by Working Group 4 participants when discussing defending intellectual property:

- It may be helpful to conduct a **risk-mapping exercise** to identify the precise risks various stakeholders face in relation to defending intellectual property.
- Stakeholders should conduct a **gap analysis** – including based on various existing texts (including existing law to manage IP theft) – to identify whether gaps exist in relation to defending intellectual property and if so, how many gaps there are, how significant they are, and whether they need to be filled (a cost-benefit analysis).
- It may be helpful to **draw from various sources of international law to give companies a more articulated apparatus** to defend intellectual property.
- Efforts to engage states and other stakeholders should recognize that **even threats of certain acts can qualify as violations of international law**.
- **Scale and proportionality of the reaction matters**. States may turn a blind eye toward certain IP theft – such as students potentially photocopying textbooks. Some activities may not be a cause of much concern if they are at a small scale – that said, it is important to acknowledge that there is a risk of escalation, especially in larger-scale IP theft.

Recommended reading & resources shared by participants

- Agreement on Trade-Related Aspects of Intellectual Property Rights (WTO): https://www.wto.org/english/docs_e/legal_e/31bis_trips_01_e.htm
- Paris Convention for the Protection of Industrial Property (WIPO): https://www.wipo.int/treaties/en/ip/paris/
- G20 Antalya Summit 2015 Communique: https://www.consilium.europa.eu/media/23729/g20-antalya-leaders-summit-communique.pdf

The Importance of Dealing With Intellectual Property Theft

Principle 4 of the Paris Call targets the protection of intellectual property in whatever form from cyberspace intrusion aiming at "stealing" it from the legitimate owners. As such, the legitimacy of the Principle cannot be disputed and, while there can be some discussion on what is exactly meant by the word "theft", everybody understands what Principle 4 talking about. Translating Principle 4 in concrete and operational actions may prove, however, to be more difficult and this for a number of reasons.

- First, the "theft" may happen without knowledge of the victim;
- Second, the magnitude of such "theft" may be difficult to assess;
- Third, the author and/or ultimate beneficiary are not easy to identify;
- Fourth, the damage may not always be easy to assess and quantify;
- Fifth, the remedies are not always actionable in particular if this requires a judicial action in the country "at the origin of theft".

That is why Principle 4 is cleverly focused on the "prevention" of the theft, i.e., to avoid the theft ex-ante rather than addressing it ex-post (to note that the word in French is "empêcher" which means both prevent and avoid). Given that the focus of Principle 4 is on prevention rather than on remediation this should draw to the logical conclusion that one should look more at technological solutions rather than at legal ones. This is not to say, though, that legal tools should not be further assessed and used as appropriate. For that a mapping of the international legal framework and a gap analysis would appear to be a key step as you can't fix what you don't know is broken!

Nicola Bonucci
Partner, Paul Hastings LLP,
former General Counsel at the OECD

Paris Call Principle #5

Non-proliferation

Digital transformation and global tensions mean that cyber risks are also high and will remain so in the future as well. In the World Economic Forum Global Risks Report 2021 the risk of cybersecurity failure was perceived high both in its impact and likelihood. Moreover, the Securing Our Digital Future report compiles statistics on global state-sponsored cyberattacks and shows how they have risen since 2005, and they continue to rise. Clearly, both the cost of cybercrime, and the numbers of attacks on victims and society are growing.

Paris Call Principle #5 on non-proliferation calls for developing ways to prevent the proliferation of malicious software and practices intended to cause harm.

There are a number of references in key international documents to the principle of non-proliferation in the ICT realm. Although non-proliferation, and related deterrence, are traditionally concepts more often referenced in the context of physical weapons of mass destruction (nuclear, biological and chemical weapons) the Working Group discussion noted that there might be elements from those approaches that could nonetheless be helpful when addressing threats emanating from cyberspace. That said, the group also acknowledged that there are significant differences that can make comparisons between the physical and cyber realms challenging and, at times, non-applicable.

The UN Group of the Government Experts (GGE) 2015 report outlines several key considerations on this topic: "States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions." This principle was reiterated in the UN OEWG 2021 report and the UN GGE 2021 report, and similar principles were laid down by the Global Commission on Stability in Cyberspace 2019 report.

In the Working Group discussion many participants highlighted that coordinated vulnerability disclosure (CVD) is a key aspect of non-proliferation. It was also recognized that CVD is not always simple and it is hard to get it right. Various CVD guidelines, tools and even standards exist, however, their adoption is insufficient and needs to be encouraged. It is also important to identify other efforts to help non-proliferation, like supporting legal initiatives and developing export control regimes.

Below are the key recommendations made by Working Group 4 participants when discussing non-proliferation:

- It is important to recognize that **coordinated vulnerability disclosure (CVD)** is a key aspect of non-proliferation.
- Though **CVD guidelines and tools** exist, **adoption** is inadequate and needs to be encouraged. To this end:
  - Additional and more effective communication is needed to **promote awareness** regarding the existing guidelines and tools.
  - **Legal barriers and uncertainty** on the matter should be addressed through national legislatures and harmonization efforts at the EU and global level.
  - **Communication with system managers** should be adequate and prompt. Recognizing that CVD lies at the core of security governance can help achieve this.
  - It is important to reach out to **people on the ground** – those actually providing the relevant services – and **encourage them to act proactively** on CVD as they are the service providers, rather than wait to be required to do so by the government or others.
  - At some point, a **"carrot and stick" approach** may also be needed, whereby inadequate CVD is met with sanctions. Illustratively, data protection started being taken much more seriously when the GDPR was implemented as it imposed significant fines, unlike some pre-existing frameworks.
- Though CVD is an important part of non-proliferation, there is significant work needed in that area – so it is also important to identify other, **low-hanging fruit** to help non-proliferation efforts. This could include, for example, supporting some technology companies' legal initiatives aimed at non-proliferation.
- It may be helpful to develop some kind of **social responsibility index** for vendors of cyber tools, to help foster accountability in relation to non-proliferation.
- It may be helpful to draw relevant lessons **from frameworks pertaining to physical weapon non-proliferation**, but it is important to recognize that certain characteristics of cyberspace make the comparisons between the physical and cyber realms challenging.

Recommended reading & resources shared by participants

- World Economic Forum 2021 Global Risks Report: https://www.weforum.org/reports/the-global-risks-report-2021
- Securing Our Digital Future: https://securingourdigitalfuture.com/
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context International Security (2015 Final Report): https://undocs.org/A/70/174

The Importance of Due Diligence in Cyberspace

The due diligence duty is a well-established concept in international law and is best summed up in the International Court of Justice's 1949 Corfu Channel decision that it is 'every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States'. In addition to this general duty, there are specialized regimes laying out due diligence duties, for example in environmental law.

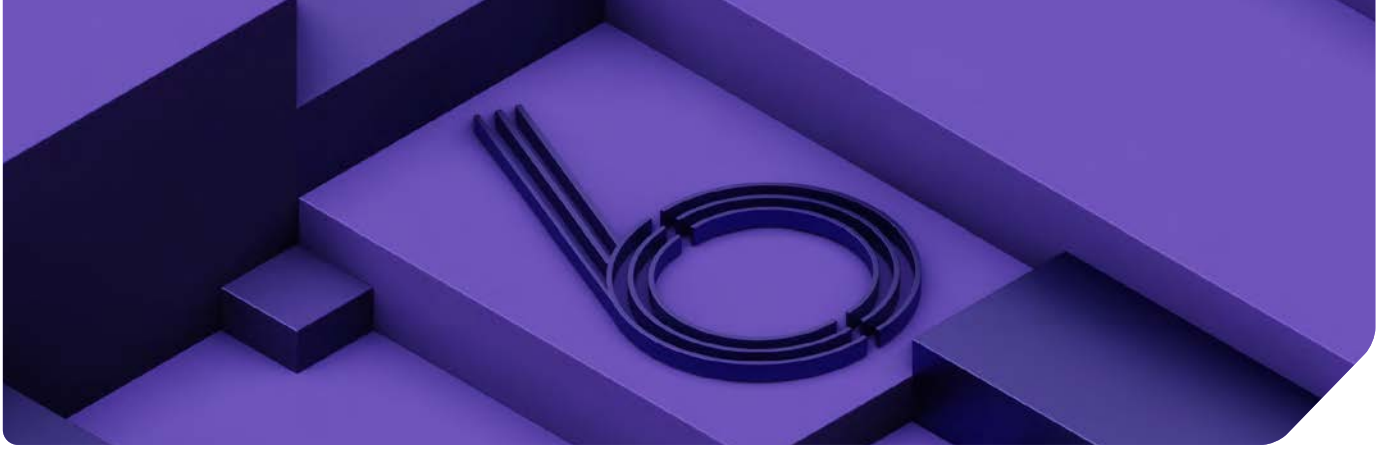
Since due diligence has been particularly effective in promoting legal developments in recent decades, it has been a prominent part of the discussions about cyber norms from the very beginning. So does the general due diligence duty apply in cyberspace, and what measures does it require states to take? While many European and Latin American States have confirmed due diligence in cyberspace, others would not publicly confirm its existence.

The 2015 UN GGE report that has been endorsed by the G7 and the G20 says that 'states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs' but avoids the word 'must' that would indicate a binding duty.

The 2021 GGE report maintained this wording while the final report of the UN OEWG does not mention due diligence at all. As for the scope of the norm, the well-respected Tallinn Manual 2.0 discusses a variety of actions states could take to fulfil their due diligence duty such as monitoring their systems for malware threats or strengthening their incident response capabilities. Yet, it explicitly rejects the idea of them being binding requirements. The drafter insist that states have a duty to take 'all reasonably available measures' to prevent their networks being used to harm others but conclude that 'the precise scope of action required by the due diligence principle is unsettled.'

Since the due diligence concept was developed to resolve or prevent conflicts between states, the international community should seek clarity as to what states can expect from each other to prevent their ICT networks being used to harm others as an urgent priority.

Jan Lemnitzer
Assistant Professor, Department of Digitalization,
Copenhagen Business School



Paris Call Principle #6

Lifecycle security & supply chain security

In recent years, sophisticated government actors have repeatedly targeted the ICT supply chain to carry out attacks, including by exploiting routine software update processes. The latter, in particular, threatens public trust and confidence in technology as update mechanisms underpin the security and maintenance of many digital products and services.

The Nobelium operation from December 2020, which compromised the supply chain of SolarWinds and impacted roughly 18,000 users, is an attack that demonstrates that international rules need to be further clarified. The operation's broad scale garnered attention from policymakers around the world, demonstrating that action to reign in these types of attacks is needed, and that it is needed sooner rather than later.

While commitments at the international level for supply chain security exist, they are often limited in scope and lack clarity in terms of application. As such, much work remains to be done by the international community and by all relevant stakeholders – especially given the complexity of the challenge.

Below are the key recommendations made by Working Group 4 participants when discussing supply chain and lifecycle security:

- **Fundamentally, international cooperation is key**, as one country could learn from the experiences of another. Additionally, it is essential to adopt a multistakeholder approach that involves not just governments but also the private sector, think tanks, academia, and civil society.
- A **risk-based approach** – that identifies risks and assesses them, including whether to undertake them – is helpful. However, the approach has its limitations. For example, consumers do not assess risk themselves. They "externalize" risk assessment – they believe minimum government standards are in place to ensure that their purchases are secure. This relates to information symmetry; consumers often lack the information required to understand a product and compare it with other products. Increased transparency, including through **certifications and labels**, can help.
- However, certifications and labels represent assessments at a given moment; **continuous assessments** would be more helpful. Further, it may not be possible to certify a product for all possible uses. It may be helpful to explore possible

The Importance of Managing Vulnerabilities

Digital transformation implies an impressive pace in terms of development of products and services, partial automation of decision-making and emerging threats. The security of digital innovations is, thus, becoming a primary concern for organizations and individuals alike. Digital products and services are pervasive - and so are vulnerabilities affecting them. Vulnerabilities are weaknesses in code, hardware, and information systems. Such loopholes are a significant source of a digital security risk as they can be exploited, thus disrupting business and social activities and harming individuals. Cybercriminal and State-sponsored actors use vulnerabilities to steal money, personal data, trade, and State secrets; disrupt operations; and hold ransom firms, cities, and hospitals. Thus, both unknown and known but unpatched vulnerabilities require appropriate management for reducing digital security risks. Vulnerability management is as much a technical as it is a business challenge. Timeliness and efficiency in managing vulnerabilities are critical to a successful digital transformation and customer trust. Thus, every organization should be responsible and accountable for effective vulnerability management. The latter includes discovery, management (patch development and dissemination) and public disclosure to enhance security knowledge and facilitate protection.

Clear guidelines for reporting potentially unknown or harmful security bugs to the proper person or team responsible (vulnerability owner) exist. Those guidelines are strengthened by numerous lawmaking initiatives that aim to enforce vulnerability disclosure, thus helping remove legal barriers and uncertainty around how to handle unsolicited yet valuable reporting of vulnerabilities from third parties. Such an optimistic development should not preclude that little attention is drawn to the shared responsibility and accountability of vulnerability proliferation through grey brokers and, more generally, insufficient patching strategies. If we were to adopt a whole-of-society approach to decreasing digital risk through effective vulnerability management, the accountability of vulnerability owners should come first. In hindsight, the longer a vulnerability is unfixed, the greater its value. The emphasis of forthcoming efforts by stakeholders should thus be on promoting and enforcing vulnerability patching as an effective approach to sustainable digital risk management.

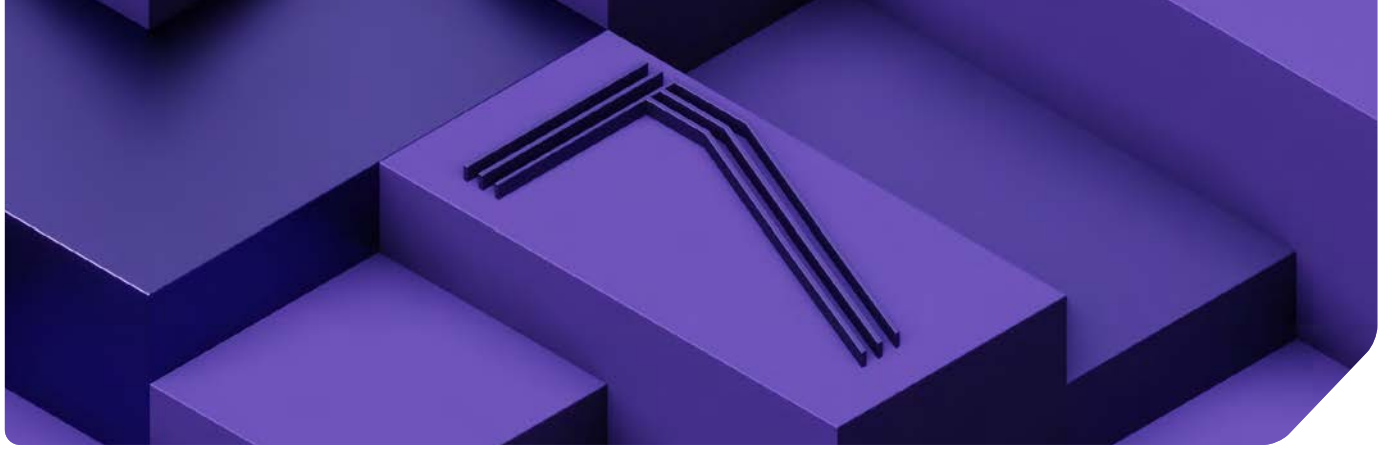
Rayna Stamboliyska
RS-Strategy Consulting

lessons from the financial sector in this regard, aimed at helping customers assess the potential risk of a product.

- It may be efficient to develop **common approaches and resources** – i.e., those that can be used by multiple companies when they assess risk, rather than each company relying on its own approach and resources. For example, multiple companies could rely on one trusted partner to verify their products, thereby eliminating the need for each company to itself conduct verifications. Notably, a trusted group of healthcare companies already share information with each other regarding threats and best practices; consolidating and distilling such information into norms could be helpful.
- More generally, leveraging **views from different industries** is important. For example, the chemical sector could provide important lessons. In that sector, regulations often require that manufacturers and integrators show customers the product's components.
- It may be helpful to **distinguish between IT requirements and OT (operational technology) requirements**. The two may merit different types of norms, standards, and transparency mechanisms.
- It may be helpful to develop a norm on **vulnerability disclosures**. Too many large organizations just deny the existence of vulnerabilities and so claim they do not need a disclosure policy. That is bad practice. Good practice would be to acknowledge vulnerabilities and invite security researchers and others to disclose them in a coordinated manner.
- It is important to think **beyond "security by design."** Policymakers often consider that a silver bullet. It is not. It is a good first step, but the entire life cycle must be considered, including policies relevant to a product's "end of life," a particularly vulnerable stage because newly discovered vulnerabilities at that stage may not be fixed by security updates if users do not implement such updates. The Internet of Things (IoT) space may be particularly at risk of this issue. Though **calls are emerging for "security by design,"** often they **are lacking for other key "duty of care" pillars** (such as security by default; vulnerability treatment; security of the organization / supply chain; and responsible end-of-life policies).
- It may be important to explore **governments' obligations and restraints** in the supply chain space, rather than focus only on those of the private sector.
- Much effort is needed on **capacity-building**, not just with small and medium size enterprises but also big organizations. Merely setting standards etc. is insufficient – "just asking for something doesn't mean it will be there."
- It is important to **allocate responsibility** more clearly, throughout the entire chain of command.
- It may be helpful to think of ways to ensure **healthy competition** because, for example, in a market with just one player, transparency may not help much.

Recommended reading & resources shared by participants

- OECD Report on Understanding the Digital Security of Products – an in-depth analysis: https://www.oecd.org/sti/ieconomy/understanding-the-digital-security-of-products-abea0b69-en.htm
- Report on Enhancing the Digital Security of Products – a policy discussion: https://www.oecd.org/digital/ieconomy/digital-security/
- The Charter of Trust: https://www.charteroftrust.com/
- OECD policy brief: Smart policies for smart products. A policy maker's guide to enhancing the digital security of products https://www.oecd.org/digital/smart-policies-for-smart-products.pdf
- OECD home page for Digital Security https://oe.cd/security



Paris Call Principle #7

Cyber hygiene

Increasing connectivity and advancements in digital technologies continue to make cyberspace increasingly central to virtually every aspect of people's lives. And even though this has brought many benefits, there is another side to this story. Specifically, these developments have been accompanied by increases in both frequency and impact of cyberattacks, putting at risk the benefits of the aforementioned advancements. Perpetrators of cyberattacks vary, as do their motivations. Cybercriminals engage in them for mainly financial gain whereas States may be involved for reasons of espionage or to further geopolitical ambitions. The good news is that measures to protect against cyberattacks do not need to consider the motivation of the attacker – rather they should focus on making the system in question more resilient and better protected. And even though it may be impossible to always protect against every threat, organizations can still significantly improve their security posture by educating their user base on best practices for secure digital engagement.

A key pillar of such considerations is cyber hygiene.

Promoting better cyber hygiene among organizations, governments and individuals is an essential part of improving an organization's security posture and it is central to protecting users and customers everywhere. It is critical that companies ensure that they implement cyber hygiene best practices in their daily operations, support like-minded organizations in the promotion of effective cyber hygiene protocols, and launch and support initiatives that raise consumer awareness.

Importantly, considering contemporary levels of connectivity, these challenges can no longer be a concern for cybersecurity professionals alone. Protecting the online environment is in everyone's interest, and must therefore be a shared responsibility. In other words, it is a multistakeholder responsibility.

This means that everyone must hold themselves accountable for adhering to cybersecurity best practices; no individual, business, government or civil society entity can be solely responsible nor fully exempt from helping to keep the internet operational, safe and secure.

Below are the key recommendations made by Working Group 4 participants when discussing cyber hygiene:

- To meaningfully improve cyber hygiene at scale and in a sustainable manner, it is essential to **adopt a multistakeholder approach** that involves not just governments but also the private sector, think tanks, academia, and civil society as appropriate.
- It is important to **identify –and build towards consensus – what the elements** of cyber hygiene are. Relatedly, when discussing implementation of cyber hygiene principles, stakeholders should be very clear about **who** (including whether it's governments, industry, or civil society organizations) should implement **what** and **how**.
- Relatedly, stakeholders should **avoid defining cyber hygiene only in terms of individual users' responsibilities**. Relying on users means relying on people's personalities which is risky and has not worked so far. Recommendations for all stakeholder groups should be developed. For instance, a duty of loyalty could be placed upon those in a position of power – such as States or companies – to act in the best interests of those who trust them.
- It is important to **develop resources describing cyber hygiene best practices** and tailoring them to all relevant **stakeholder groups** including manufacturers, organizations, and consumers. These resources should be **simple to understand** and need not be limited to the written form; they can include video. It is also important to ensure these resources are **widely disseminated** among their target audiences.
- Relatedly, there should be **one or multiple centralized hubs** responsible for providing and maintaining guidance on cyber hygiene, like guidance on public health issues in the U.S. can be found on the Centers for Disease Control (CDC) website. With such centralization, users and other stakeholders will know where to easily find reliable, updated information on cyber hygiene. Stakeholders should give some thought to which actors might comprise these hubs for cyber hygiene, or how the right actors can be identified.
- Awareness should be raised around **minimum standards for any internet user** – aspects of which could include, inter alia, **multi-factor authentication** (the entry point for cyberattacks is often stolen credentials, so multi-factor authentication can help prevent common attacks like phishing and password spray); HTTPS-only web access; DKIM (DomainKeys Identified Email) records in incoming/outgoing email; secure home routers; and standards related to Internet of Things (IoT) devices (given how common such devices are becoming in people's homes).
- Similarly, awareness should be raised around **best practices for citizens** – e.g., changing passwords frequently; not giving away certain information in certain situations; open Wi-Fi restrictions; avoiding IoT devices if not necessary; remote mobile phone detection; etc.
- It is important to consider **whether *voluntary* cyber hygiene is enough**, especially given some of the more recent attacks that have been occurring, including on healthcare organizations and the supply chain in general.

Recommended reading & resources shared by participants

- The Cyber Security Tech Accord: https://cybertechaccord.org/
- The Cyber Security Tech Accord's Compendium on Cyber Hygiene: https://cybertechaccord.org/uploads/prod/2020/11/Cyber-Hygiene-Appendium-update-191120-pages.pdf

Guidance from the Cybersecurity Tech Accord on Paris Call principles #7 and #8.

One of the great benefits of the Paris Call is that is pulls together a global community of supporters to promote peace and security online, which is important because this is a multistakeholder challenge. As part of this community, the Cybersecurity Tech Accord – a coalition of more than 150 global technology companies – sought to provide implementation guidance related to principles where it has unique expertise in twin publications released in 2020, one focused on principle #7 (cyber hygiene) and the other on principle #8 (no private hack back).

The Cyber Hygiene Compendium

This compendium serves as an easy-to-navigate guidebook with concrete steps to improve cyber hygiene for individuals and organizations alike, reflecting guidance from across Tech Accord signatories. It features best practice guidance on a range of topics, including multifactor authentication, domain name security, email authentication, routing security, virtual private networks, and how to defend against common attack methods like password spray.

No Hacking Back: Vigilante Justice vs. Good Security Online

This whitepaper provides a deep dive into what is considered inadvisable and illegal "hack back" activities versus valuable forward-leaning security practices employed by the technology industry today. It serves as an essential guide for policymakers seeking to better understand the boundaries of industry actions in cyberspace to prevent and deter cyberattacks by criminals, and why "hack backs" are not a suitable way to address the increasing number of threats.

Annalaura Gallo
Associate Director, APCO Worldwide

Paris Call Principle #8

No private hack back

Threats emanating from cyberspace continue to increase, impacting individuals, industry and the international community of States. That said, they often cause particularly significant damage to the private sector. Increasingly this has resulted in discussions whether and how private sector entities may respond to these developments, including whether a potential response might also consist of retaliatory actions.

The Paris Call addresses this and contains a commitment to prevent the private sector hack back. To provide context, and as noted by the Cybersecurity Tech Accord, this term, "hack back," is generally understood to refer to offensive actions by private sector organizations – i.e. independent of governments – in response to a cyberattack in order to either steal back from, or otherwise cause harm to, the computer systems or networks of attackers – in other words, retaliatory hacking, often violating criminal and civil legal obligations in the process.

Paris Call principle #8 discouraging such behaviors is essential to a rules-based international order in cyberspace where it acknowledges that, just as in the physical realm, governments must play a leading role in enforcing laws and holding criminals accountable – while also taking into account the role other stakeholders and especially industry play in this space.

Unfortunately, however, defining an abstract concept as "hacking back" is challenging. To respond to an ever-changing threat environment, the private sector, especially the technology industry, needs to continuously innovate to create more effective security measures.

As the majority of cyberspace is owned, operated and maintained by private industry, many of the actions taken by government agencies and law enforcement groups against malicious actors online inevitably require the private sector to comply with legal demands and process. In some cases, governments and industry may even co-ordinate action to disrupt malicious actors online. What this means is that as decision- and policy-makers consider such actions, they do so with restraint and precision, or – as noted by the Cybersecurity Tech Accord, "with a scalpel, as opposed to a hammer" – so as to avoid encouraging escalatory and dangerous hack back activities, while at the same time not inadvertently prohibiting measures that have become important in maintaining good security, and leaving space for continued innovation in security practices by the private sector.

Below are the key recommendations made by Working Group 4 participants when discussing private hack backs:

- To meaningfully tackle the threat of private hack back, it is essential to **adopt a multistakeholder approach** that involves not just governments but also the private sector, think tanks, academia, and civil society, as appropriate.
- It is important to **recognize nuance in defining hacking back** so that stakeholders don't discourage responsible security practices. For example, the Cybersecurity Tech Accord adopted such an approach in reaching its definition of hacking back: "unauthorized access to a protected computer or network by individuals or organizations, following an attack, in order to steal data or otherwise harm an attacker." This definition helps protect a range of appropriate active defense measures which would target an ongoing attack, but which largely or entirely take place in environments that are owned or operated by an organization or their customers with consent. The definition also helps protect legally legitimate actions.
- Relatedly, in efforts to prevent hack back, policymakers should avoid broad prohibitions as they could stifle **innovation** in security practices. Innovation ensures security practices keep pace with attacker behavior.
- Stakeholders should **avoid looking at the issue of hacking back from an individual user's perspective** – hacking back can seem to be a more justifiable response when viewed from such a comparatively narrow perspective.
- It is important for stakeholders to recognize that a major downside of hacking back, other than potential escalation and the potential illegality of the conduct, is the substantial chance of it causing **collateral damage** on innocent parties. Smart hackers may route their attacks through innocent parties' networks and any retaliatory attack is likely going to hit those networks as well.
- States should not use companies for hacking back. Some jurisdictions have proposed versions of **"private hack back"** or a letter of marque parallel, which would authorize certain groups to hack back – largely out of frustration fueled by recent attacks. In other words, even though such hacking back would be government-sanctioned, it is nevertheless inappropriate. Similarly, companies should not offer **"hack for hire"** services – to be used by States or other non-State actors – for hacking back.
- Relatedly, any effort to take down botnets should be conducted in **coordination with – and under the leadership of – government actors, such as law enforcement agencies** with appropriate investigative power. Coordinating with them will help make sure the effort is within legal boundaries and will help mitigate interference with ordinary people's computers.
- Preventing hack back may require a **cultural change**, as the IT industry has a history of self-policing (e.g., blacklisting organizations sending spam emails). Relatedly, popular culture including Hollywood sometimes glamorizes hacking and hacking back, thereby making efforts to prevent hacking back harder. It is therefore important to ensure stakeholders distinguish popular culture from reality.
- Efforts to prevent hack back should draw, as appropriate, from ongoing efforts at the UN in relation to **cyber mercenaries**, as there may be an overlap between the two efforts.

Recommended reading & resources shared by participants

- "No hacking Back: Vigilante Justice vs. Good Security Online" – A Policymaker's Guide to Knowing the Difference (report by the cybersecurity Tech Accord): https://cybertechaccord.org/uploads/prod/2020/11/hack-back-update-131120-pages.pdf
- The Cyber Security Tech Accord: https://cybertechaccord.org/
- A Duty of Loyalty for Privacy Law: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3642217
- Private actor cyber defense and (international) cyber security – pushing the line?: https://academic.oup.com/cybersecurity/article/7/1/tyab010/6199903

Paris Call Principle #9

International Norms

Paris Call principle #9 is about international norms. Its aim is to "promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace."

There are several international initiatives that support the objectives of this principle, such as the Confidence-Building Measure (CBM) catalogue of the Organization for Security and Co-Operation (OSCE). For example, one key CBM focuses on the creation of a point of contact (PoC) network to help States in facilitating information on ICT-related incidents. Also noteworthy is the Internet Governance Forum's (IGF) 'Best Practice Forum Cybersecurity on the use of norms to foster trust and security'. The intention is to take a deeper look at the drivers of cybersecurity norms and test these concepts against historical experiences, to better understand how specific norms can be effective in mitigating adverse cybersecurity events.

In the discussion it was noted how complex the stakeholder ecosystem around cybersecurity norms is. Diplomats at the UN and in regional organizations discuss modalities for existing and new norms. A variety of stakeholders, such as Global Partners Digital, the Global Forum on Cyber Expertise (GFCE) support the practical implementation of agreed norms. Multistakeholder initiatives such as the Global Commission on the Stability on Cyberspace, or private stakeholders like Microsoft contribute through the development of new and further refinement of existing norms. Academics analyze the impact of norm development and implementation. Moreover, many of the beforementioned stakeholders are engaged in additional ways of norm discussions.

The Working Group therefore decided to focus on sharing best practices around norm implementation, as well as on how to leverage the Paris Call community to connect and reinforce the various cybersecurity norm efforts.

Below are the key recommendations made by Working Group 4 participants when discussing international norms:

- To help prevent and respond to cyberattacks, States should share information regarding cyber threats and incidents not just with each other but also with other relevant stakeholders, including companies operating in critical infrastructure sectors, such as healthcare.
- It is also important for private companies to better share information with each other, and throughout the industry verticals.

- It would be helpful to have more formalized cooperation between regional organizations than currently exists.
- Stakeholders should not see norms' non-binding nature as particularly limiting; norms are still a political commitment and when a country violates a norm, it is fair for other countries and stakeholders to hold the violating country accountable.
- Though what is perceived as responsible State behavior may shift according to the political positioning of State leaders, continuous formal and informal dialogue among States and other key stakeholders – people sitting at one table – can help maintain cyber peace and stability.
- Multistakeholder organizations, such as the GFCE, should view the UN reports as a strong foundation for engaging in and strengthening capacity building efforts; Recent United Nations reports highlighted the importance of such efforts as a foundational pillar to international cyber stability.
- States should consider expanding support to capacity building entities such as the GFCE; for example, statements of support from high-level individuals and platforms like the Paris Peace Forum and the Paris Call for such work can be very helpful.
- It is important to consider capacity building as foundational to the UN Sustainable Development Goals. The GGE and OEWG reports did not do so, as they likely saw it as beyond their mandate. But it is not beyond the mandates of other platforms such as the Paris Peace Forum, to advance messaging and encourage commitments to this effect.
- Another option to consider and explore would be the possibility of stakeholders, including states, opening themselves up to peer reviews – e.g., states rating neighboring states or continents in terms of their norms compliance – to help foster best practices and trust.

Recommended reading & resources shared by participants

- UN OEWG Report 2021: https://www.un.org/disarmament/open-ended-working-group/
- UN GGE Report 2021: https://www.un.org/disarmament/group-of-governmental-experts/
- Overview of OSCE Cyber CBMs: https://www.osce.org/secretariat/cyber-ict-security
- Internet Governance Forum (IGF) 'Best Practice Forum Cybersecurity on the use of norms to foster trust and security: https://www.intgovforum.org/multilingual/content/bpf-cybersecurity
- Global Partners Digital: https://www.gp-digital.org/
- The Global Forum on Cyber Expertise (GFCE): https://thegfce.org

Advancing International Norms

CCSIRS (Center for Cyber Security and International Relations Studies)
Luigi Martino, Luigi lo Porto, Dania Di Giusto, Nada Gamal

Research Project Summary

Introduction and Research Background

Cyberspace plays a key role at the economic, political, military and social level. It has also become a relevant part of the international system. The role of the new cyber frontier has become significant for the way that States conceptualize their interests in the contemporary world. The comparatively low barrier of access to Information and Communications Technologies (ICTs) capabilities incl. offensive capabilities, the speed of technological advances and the complexity of the comparatively ungoverned cyber domain with regard, for instance, to traditional legal definitions of national borders, have presented new challenges to States that can cause potential and unaddressed geopolitical tensions. These can arise from the inherent complexity of accurately attributing cyber-attacks targeting essential services and critical infrastructures or from a lack of defined red lines, when it comes to deterrence. In addition, limiting malicious activities in cyberspace is important for protecting international peace and stability and that can only be assured through diplomacy, as many analysts and policymakers agree. From this perspective, we need to be able to move collectively, involving public and private stakeholders, as well as the research communities, given that diplomacy an exercise in the domain of solely the diplomatic staff of one nation and that of another, but also between IGOs, NGOs, private companies, national actors and civil society. For instance, international and regional actors such as the United Nations (UN), Council of Europe, the Organization for Security and Cooperation in Europe (OSCE), the G7 and the Organization of American States (OAS), have launched specific initiatives to enhance stability, improve cooperation, and increase trust and transparency among states in the cyber arena. These initiatives include, in general, the identification of common norms for responsible state behaviour, confidence building measures, capacity building measures (to bridge the digital gap) and, in particular, operational measures needed to reduce the risk of misperception, military escalation and political tension in cyberspace. What is missing is a tool able to read, analyse and compare in a dynamic way the main practical results of international efforts to govern cyberspace. For this reason, the Center for Cyber Security and International Relations Studies (CCSIRS) set up a research project whose final objective is the creation of such a dynamic tool, which would automatically update, leveraging several data sources (primary and secondary, including literature review) and which would compare issues and contents of the most relevant cyber diplomatic initiatives undertaken to regulate the cyber domain. This instrument would facilitate the implementation of the most effective cyber diplomatic and normative tools and increase the overall international stability.

Research Methodology

The research method is based on a qualitative comparative approach (QCA). The analysis provides an overview of the current state of desk research-examined empirical data, including all relevant global actions and initiatives, with a particular focus on diplomatic and normative measures in cyberspace at bilateral[1], multilateral[2], regional and international levels. A critical analysis of case studies and practices draws out the basic elements of effective cyber diplomatic initiatives. Over the recent years, a significant acceleration of diplomatic efforts in the cyber field was evident from the broad range of initiators and stakeholders engaged, including international organizations. The data collection, based on available open data sources[3], has been articulated in key findings and classified in different categories, such as country/economic area, diplomatic initiatives (date of issue and state of implementation), normative initiatives (date of issue and state of implementation), description of the measure, party proposing the measure. The result is a dynamic dataset that compares outcomes thanks to established functional and performance requirements, identifies good practices of cyber diplomacy and how widely they are used, as well as the challenges, obstacles and limitations to their use. It then links it to the Paris Call principles, based on a specific taxonomy built around a conceptual and analytical framework. We recognize that the latter needs to be improved further by soliciting feedback, consulting with a wider expert community and disseminating the outcomes.

Gap Analysis

Taking into account the goal of the Paris Call Working Group 4, the CCSIRS began to set up current frameworks corresponding to the 9 Principles of the Paris Call. What immediately emerged is the effectiveness of confidence-building measures (CBMs) as they have been developed by several actors, in particular the United Nations Group of Governmental Experts (UN GGE) 2013, 2015, 2021 Reports, the Open-ended Working Group (OEWG) 2021 Report[4], the G7 Carbis Bay Summit Communiqué (2021)[5], the Organization for Security and Co-operation in Europe (OSCE) 2013 11 CBMs and the 2016 5 CBMs[6], the Association of South-East Asian Nations (ASEAN) Regional Forum Work Plan on Security of and in the Use of ICTs (2015),[7] the ASEAN 2018 Leaders' Statement on Cybersecurity Cooperation[8], the 13th ASEAN-Japan Cybersecurity Policy Meeting in 2020[9] and the 2020 Agile Nations Agreement advanced by the Organization for Economic Co-operation and Development (OECD) and the World Economic Forum[10]. Confidence-building measures are expected in the Principle 9 of the Paris Call alongside international norms of responsible state's behavior[11]. For instance, States are recommended

1 Analysis of bilateral dialogues, initiatives and agreements by the following actors: U.S. – Russia dialogue, U.S. – China dialogue, Russia – China, Russia – India, Russia – south Africa agreements, U.S. – India framework.

2 Assessment of multilateral initiatives by the following actors: United Nations, Organization for Security and Cooperation in Europe (OSCE), Association of Southeast Asian Nations (ASEAN) Regional Forum, Shanghai Cooperation Organization, BRICS, North Atlantic Treaty Organization (NATO), Group of 20, Group of 7, Organization of American States.

3 I.e.: the NATO CCDCOE (Cooperative Cyber Defence Centre of Excellence) research tool International Cyber Developments (INCYDER), **https://ccdcoe.org/research/incyder/**; the UNIDIR (United Nations Institute for Disarmament Research) Cyber Policy Portal, **https://unidir.org/cpp/en/**; the International Cyber Law Toolkit developed by the Czech National Cyber and Information Security Agency (NÚKIB), **https://cyberlaw.ccdcoe.org/wiki/Main_Page**; the Cyber Norms Index and Timeline of the Carnegie Endowment for International Peace, **https://carnegieendowment.org/publications/interactive/cybernorms?mkt_tok**; the Cyber Conflict Portal (CCP) of the EU Cyber Direct, **https://eucyberdirect.eu/content_research/cyber-conflict-portal/**; the DiploInCyber project which is launched by the CCSIRS to initiate the research and create an independent database to assemble the information and provide easy access to each document, **https://www.cssii.unifi.it/vp-162-diploincyber.html**; the Global Cybersecurity Index of the ITU (International Telecommunication Union), **https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx**; the National Cyber Security Index (NCSI) of the e-Governance Academy, **https://ncsi.ega.ee/**.

4 UN, "Developments in the field of information and telecommunications in the context of international security", n.d., **https://www.un.org/disarmament/ict-security/**.

5 G7, Carbis Bay G7 Summit Communiqué, June 13, 2021, available at: **https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/**.

6 OSCE, "OSCE participating States, in landmark decision, agree to expand list of measures to reduce risk of tensions arising from cyber activities", osce.org, March 10, 2016, **https://www.osce.org/cio/226656**.

7 UNIDIR, "Association of Southeast Asian Nations (ASEAN)", n.d., **https://unidir.org/cpp/en/organization-pdf-export/eyJvcmdhbml6YXRpb25fZ3JvdXBfaWQiOiIyIn0**.

8 Ibid.

9 Ibid.

10 OECD, "'Agile Nations': Nations Sign First Agreement to Unlock Potential of Emerging Tech", December 9, 2020, **https://www.oecd.org/gov/regulatory-policy/agile-governance-for-the-post-pandemic-world-wef-oecd-joint-event.htm**.

11 The UN Security Council Arria-formula Meeting: Cyber Stability, Conflict Prevention and Capacity Building (2020) treats about international norms of responsible state's behavior.

to protect critical infrastructures (Principle 1), in accordance with the UN Security Council Arria-Formula meeting: Cyber Attacks Against Critical Infrastructure (2020), the 9th ASEAN-Japan Information Security Policy Meeting in 2016[12] and the Organization of American States (OAS) Call to action to protect citizens, the private sector and the Government (2018)[13]. The UN GGE 2015 and 2021 Reports and the OEWG 2021 Report, together with the Global Commission on the Stability of Cyberspace (GCSC) 2019 Report, the ASEAN Framework on Personal Data Protection (2016) and the Commonwealth Cyber Declaration (2018) have undertaken recommendations about Principle 1 (protection of individuals, critical infrastructures and sensitive information). The UN GGE 2015 Report, the OEWG 2021 Report and the GCSC 2019 Report are additionally geared towards Principle 2 (protection of the internet and of its general availability and integrity).[14] Several diplomatic initiatives in the cyberspace have been set up to defend democratic electoral processes from attacks, coordinated manipulation and disinformation. For instance, the UN GGE 2013 Report, the NATO Tallinn Manual[15], the GCSC 2019 Report, the ASEAN Framework on Digital Data Governance[16] and the G7 Digital and Technology Ministerial Declaration (2021)[17]. In relation to Principle 3, other multi stakeholder initiatives should be mentioned. These include the Oxford Process on International Law Protections in Cyberspace, the Cyber Law Toolkit by the Czech National Cyber and Information Security Agency (NÚKIB), the International Committee of the Red Cross (ICRC), the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and other partner institutions, the 2017 Joint Declaration on Freedom of Expression and Fake News, Disinformation and Propaganda by the UN, the OSCE, the Organization of American States (OAS) and the African Commission on Human and People's Rights (ACHPR)[18]. Regarding the defense of intellectual property, trade secrets and business information from theft (Principle 4) the UN GGE 2015 Report, the G20 Antalya Summit (2015) and Hamburg Summit (2017)[19], the World Intellectual Property Organization (WIPO) Paris Convention and the Framework for G7 Collaboration on Electronic Transferable Records (2021 Annex 4 of the G7 Digital and Technology Ministerial Declaration)[20] need to be mentioned. Measures related to Principle 6 (security of digital processes, products and services throughout their lifecycle and supply chain) have been employed by the G7 Carbis Bay Summit Communiqué (2021), the G20 Antalya Summit (2015) and Hamburg Summit (2017), the 2021 Declaration of G20 Digital Ministers[21] and the European Union Agency for Cybersecurity (ENISA)'s Good Practices for Security of Internet of Things[22]. Actions that allow the non-proliferation of malicious software, hardware, practices and tools that cause harm (Principle 5) are envisaged in the UN GGE 2015 Report, the OEWG 2021 Report, the GCSC 2019 Report and the Adoption of a Comprehensive Inter-American Strategy to Combat Threats to Cybersecurity by the OAS in 2004[23]. Actions that prevent from private hack-back (Principle 8) are defined by the Cybersecurity Tech Accord[24], the EU Cyber Diplomacy Toolbox[25], the Council of Europe Convention on Cybercrime[26], the 2019 Christchurch Call by the G7[27] and the OEWG 2021 Report. Measures concerning Principle 7 (cyber

12 Ministry of Economy, Trade and Industry of Japan, The Ninth ASEAN-Japan Information Security Policy Meeting to be Held, n.d., **https://www.meti.go.jp/english/press/2016/1007_01.html**.

13 The Organization of American States (OAS) Call to action to protect citizens, the private sector and the Government (2018) also concerns Principle 4 and 6. The call is available at: **http://www.oas.org/en/sms/cicte/awswhitepaper.pdf**.

14 The report is available at: **https://cyberstability.org/report/**.

15 M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, New York, Cambridge University Press, 2013.

16 ASEAN, "Asean Data Management Framework", n.d., **https://asean.org/wp-content/uploads/2-ASEAN-Data-Management-Framework_Final.pdf**.

17 The declaration is available at: **http://www.g7.utoronto.ca/ict/2021-digital-tech-declaration.html**.

18 OSCE, "Joint declaration on freedom of expression and "fake news", disinformation and propaganda", March 3, 2017, **https://www.osce.org/fom/302796**.

19 See: **http://g20.org.tr/; http://www.g20.utoronto.ca/summits/2017hamburg.html**.

20 The 2021 Annex 4 of the G7 Digital and Technology Ministerial Declaration is available at: **https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/G7_Digital_and_Technology_Ministerial_Declaration.pdf**.

21 Declaration of G20 Digital Ministers, "Leveraging Digitalisation for a Resilient, Strong, Sustainable and Inclusive Recovery", August 5, 2021.

22 As example of report concerning good practices of cybersecurity, see: ENISA, "Good Practices for Security of Internet of Things: Secure Software Development Lifecycle", November, 2019, **https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot-1**.

23 Resolution AG/RES. 2004 (XXXIV-O/04), "Adoption of a comprehensive inter-american strategy to combat threats to cybersecurity: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity", June 8, 2004

24 For an overview, see: **https://cybertechaccord.org/**.

25 Council of the European Union, Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox"), Brussels, 7 June, 2017.

26 Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001.

27 As reported in the dedicated website: "The Call outlines collective, voluntary commitments from Governments and online service providers intended to address the issue of terrorist and violent extremist content online and to prevent the abuse of the internet as occurred in and after the Christchurch attacks". See: **https://www.christchurchcall.com/call.html**.

hygiene) are indicated in the Cybersecurity Tech Accord, the Guidelines on Child Online Protection (COP)[28] endorsed in 2020 by the International Telecommunication Unit (ITU), the G7 Internet Safety Principles (Annex 3 of the G7 2021 Digital and Technology Ministerial Declaration)[29].

Conclusion

As mentioned, the research project aims to contribute to the analysis and evaluation of the main diplomatic initiatives concerning the cyber domain. It does that through a detailed performance of criteria design, identification of underlying good practices and achievement, but also challenges and limitations of those initiatives. The outcome is envisaged as a dynamic tool, which is expected to compare content of the main diplomatic initiatives and the related measures so as to measure the effectiveness of the cyber diplomacy processes. The results so far indicate that an insufficient conformity of mapping capabilities and the risk of redundancy of norms are the main weaknesses of the diplomatic actions, undermining not only the success of the specific initiative per se but also the common aim of enhancing international security and stability in cyberspace. In our view, challenges, risks and emerging obstacles of cyber diplomacy could be overcome by reaffirming a multistakeholder approach that involves governments, industry and civil society and the complementing activities carried out by regional organizations through their integration in the relevant international fora, such as the United Nations.

28 See the COP guidelines website: **https://www.itu-cop-guidelines.com/**.

29 G7 Digital and Technology Track – Annex 3: G7 Internet Safety Principles G7 Digital and Technology Ministers, April 28, 2021, available at: **http://www.g8.utoronto.ca/ict/2021-annex_3-internet-safety.html**.

Annex A:

Outcomes of Supplementary Events

The regular meetings of Paris Call Working Group #4 focused on the nine Paris Call principles and on coming up with ideas and proposals to advance cyber security norms discussions related to these principles. To complement these discussions, throughout the year, the German Marshall Fund (GMF) and Microsoft partnered on organizing supplementary events to further support the spirit and the ambitions of the working group.

Below are the outcomes of these deliberations.

Report of May 18, 2021 meeting

Promoting Cyber Norms to Protect our Healthcare Infrastructure

Executive summary

Participants agreed that the healthcare sector is particularly vulnerable, because of the vast amount of data that needs to be processed for healthcare delivery, but also because of low barriers to entry and the potential for a significant impact. Participants also agreed that the healthcare community is currently underprepared to handle even existing risks, such as conventional cyberattacks, let alone the far more sophisticated and dangerous risks on the horizon, such as quantum attacks or attacks targeting AI and IoT technologies.

Participants agreed that various measures and approaches needed to be adopted to help protect the healthcare sector. These include a multistakeholder approach involving governments, industry, civil society, and academia as appropriate; relatedly, robust cooperation and information sharing (including on threat intel) among companies; strong cybersecurity hygiene; mobilizing investment in cybersecurity; crafting legislation to clearly address vulnerable aspects of the healthcare sector; assigning some cybersecurity responsibility to healthcare entities' management personnel; continually updating cybersecurity awareness, laws, best practices etc. to account for rapidly evolving threats; and recognizing how exactly international law applies to cyberspace in this context.

Distilled key recommendations

- It is important to adopt a **multistakeholder approach** which includes (as appropriate) government, industry, civil society, and academia. This does not mean that non-government entities should make decisions, which should be reasonably made by governments. It also does not mean that all stakeholders need to be consulted on all issues all the time. It means that when an issue is too challenging to reasonably be tackled by any one stakeholder group – as is protecting healthcare infrastructure from cyberattacks – all relevant stakeholders work together to solve the problem.

- **Cooperation among companies** has become even more crucial than before. This includes sharing threat information and best practices.
- **Cybersecurity hygiene** is critically important because digital innovation has become commonplace in the healthcare sector; in fact, the pandemic has accelerated it. Cybersecurity hygiene may include, among other things, a proper cybersecurity framework; ensuring security controls are in place; conducting effective vulnerability management – in relation to not just infrastructure but also applications; robust trainings for healthcare providers on how to protect electronic data; and designing technologies with cybersecurity in mind right at the outset. Of course, protecting data from cyberattacks should not preclude that data from being accessed and used for legitimate purposes.
- Relatedly, it is important to **mobilize increased investments in cybersecurity**. Notably, hospitals often do not have enough money to provide sustainable cybersecurity, even though medical data is just as sensitive as financial. Hospitals often spend a fraction of the amounts seen in the banking sector on cybersecurity, as they often struggle to provide even basic healthcare needs.
- Protecting **supply chains** is essential to help protect the healthcare sector, because essentially all parts of the healthcare delivery process are digitized, such as scheduling of patient appointments, medication, inpatient and outpatient care, etc. The importance of protecting supply chains is also clear from the workings of the medical device industry, where data flows through multiple transactions, such as from the hospital to the cloud, and from the product to the hospital, etc.
- **Legislation** is an important part of the solution, even though it is just one part. Countries should enact legislation to specifically protect all vulnerable facets (including entities) of the healthcare sector, rather than just the healthcare sector in general, as the latter approach may lead to confusion about whether particular facets of the sector are covered. Sectoral legislation (i.e., legislation targeted to the healthcare sector) is important, but so is horizontal or cross-sector legislation, which helps address issues common to multiple sectors. Relatedly, in **Europe**, relevant institutions could issue not just laws but also guidelines to encourage cybersecurity best practices at the EU Member State level.
- Cybersecurity awareness, laws, best practices, etc. need not only robust investment but also **continual updating** to account for rapidly evolving technology and evolving threats.
- It is important to recognize not just that international law applies to cyberspace, but also how exactly it applies. And this is true not just in relation to cyberspace in general but also to its subsections. The Oxford Process seeks to provide such clarity – by articulating points of consensus under international law on pressing global issues. Notably, the Oxford Process has produced multiple statements, two of which focus on health: one on the healthcare sector and the other on vaccine research.

Report of June 10, 2021 meeting

Promoting Cyber Norms to Protect our Supply Chain Infrastructure

Executive summary

Participants agreed on the need for a multistakeholder approach. They also noted the importance of international norms, but also highlighted that practical guidance on their implementation is needed. Similarly, they highlighted the need for awareness raising of the fact that international law obligations exist in cyberspace, but in a manner that helps implement those obligations rather than merely discussing them in the abstract. Participants also noted the importance of coordination on cybersecurity efforts at the European level, given Europe's potential role in global standard-setting.

Participants noted that companies should – as some are already doing – focus on supply chain cybersecurity at the board level; allocate substantial funds to the matter; assess suppliers' security through practical risk-based methodologies that are harmonized across companies and countries; share assessments with each other; treat supply chain cybersecurity as one way to attract consumers; and recognize that many professionals relevant to supply chain cybersecurity may be unfamiliar with cybersecurity and therefore train them accordingly.

Distilled key recommendations

- A **multistakeholder approach** is important. As appropriate, governments, industry, and civil society should work together to address challenges pertaining to supply chain security.
- Norms are important to have, and the international community should consider exploring whether a dedicated, supply chain focused norm should be elaborated in the future. In addition, **practical guidance on implementation** is essential, especially for smaller companies. The recent report of the Group of Governmental Experts provides some such guidance, but more is needed.

- **Coordination at the European level** is important to help develop robust and consistent cybersecurity best practices across the continent, which in turn is particularly important given Europe's potential role in global cybersecurity standard-setting. There are several cybersecurity efforts underway in Europe, such as rewriting the NIS directive and upcoming legislation on connected products. Relatedly, European efforts should be conducted in consultation with all relevant stakeholders, including other countries and international organizations.
- Supply chain cybersecurity issues are so critical that companies should focus on them at the **board level**, as some are already doing. Relatedly, as we are already seeing happen, companies should **allocate substantial funds** toward addressing supply chain cybersecurity issues.
- Companies should **assess suppliers' security** through practical risk-based methodologies. Such approaches should be harmonized across companies and countries. Companies should share assessments with each other so as not to duplicate efforts. However, such sharing and harmonization should not violate competition law, or create vulnerabilities in the system. Large companies should take an active role in assessing supplier security because this can help foster trust – i.e., once a large company finds a supplier trustworthy, other companies are likely to trust that supplier.
- Companies should conduct rigorous **training** for the many professionals involved in supply chains, who might not understand the issues at stake, and whose jobs will become much more challenging with the inclusion of complex cybersecurity issues.
- Companies should consider supply chain cybersecurity as one way to gain a **competitive edge** – it can make their products and services more attractive to consumers.
- It is important to find ways to **increase transparency across the supply chain**, including upstream. This can be particularly difficult for small and medium size enterprises, who should be supported in this regard.
- It is important to spread awareness about **international law obligations** that exist in cyberspace. These should not just be discussed in abstract terms; it is critical that there is more clarity as to how legal protections can be implemented. Exchanging ideas and cooperation across sectors to this end would be beneficial.

Report of September 28, 2021 meeting

Protecting Democratic Institutions and Processes in Cyberspace

Executive summary

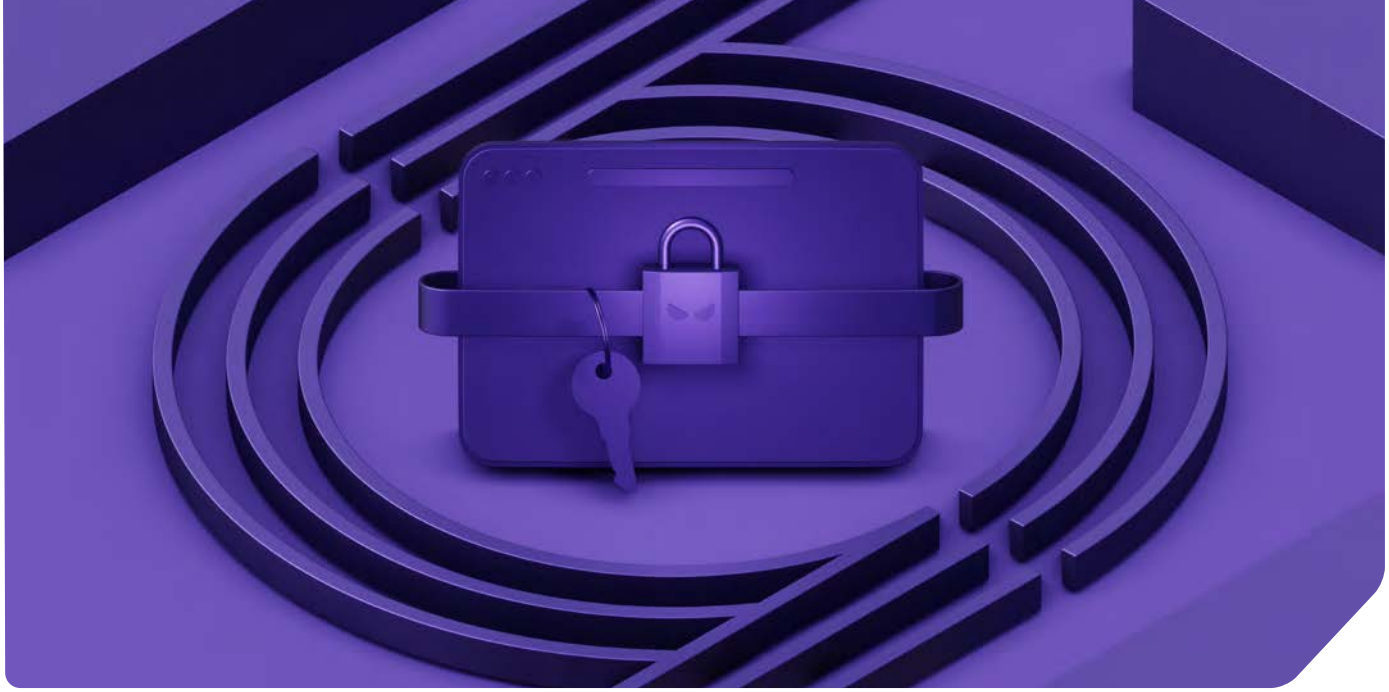
Participants agreed on various general matters regarding the ongoing conversations on cybersecurity norms, including that such discussions must firmly take into account real-world developments; try also to anticipate the kinds of (real-world) attacks that have not yet occurred but can; and focus on harms to the individual.

In relation to information operations, participants agreed on taking a holistic approach – looking not just at the attack but also at the broader dynamics – e.g., what the actor does with the information, what the messaging is, and so on. Participants also stressed the importance of careful taxonomy, including distinguishing between "disinformation" and "misinformation"; equipping people with reliable sources of information; and relatedly, the media's transparency and accuracy. In connection with international law, and to help foster positive behavior among states without creating friction, participants proposed the legal notion of liability, whereby a perpetrator state has the opportunity to remedy the harm caused; and helping states agree with each other on the specifics of how international law applies to cyberspace, work that the Oxford Process is doing.

Distilled key recommendations

- Many discussions of norms happen in the hypothetical, whereas it is important to discuss norms in the **context of real-world situations**.
- When discussing of information operations, it is important to think not only of the attack itself but also **the broader information landscape** – e.g., what the actor does with the information, whom it targets, what the messaging is, what the result of that may be, and so on.
- It is important to ensure people have **reliable sources of information** and, relatedly, **to raise awareness** among the population to make them better capable of assessing the information they receive.

- Relatedly, when reporting on cyber threats to democratic institutions and processes, **the media should be as candid, transparent, and accurate as possible**, including quoting and naming sources and experts where feasible.
- **Paper-based voting** can reduce the risk of vote manipulation. Relatedly, having paper-based options/back-ups can be a form of resilience.
- It is important for States to recognize that **merely having paper ballots need not prevent the success of disinformation campaigns designed to undermine trust in elections**. A dedicated actor with access to appropriate distribution channels may still be able to do significant damage.
- When applying international law to this issue, it is important to recognize that there is a **patchwork of international law rules that apply, not just one consolidated legal framework** like a treaty. Examples of applicable rules include the principles of non-intervention and due diligence.
- It is important to think about – such as in the context of the SolarWinds attack – when **espionage** which is traditionally permissible under international law crosses the line into being harmful and worth prohibiting.
- To encourage positive behavior among states without creating animosity, it may be helpful to:
  - consider the legal notion of **liability**, which gives a perpetrator State the opportunity to remedy the harm caused (and the admission would be of lack of due diligence rather than admitting being directly responsible); and
  - help States **agree with each other** (and with other key stakeholders) **on the "rules of the game"** – i.e., the specifics of how international law applies to cyberspace (work The Oxford Process is trying to do).
- It is important to **frame discussions in terms of the harms caused to *individuals***. That concretizes the harm. Focusing on states over individuals is less helpful, because the state is an abstract entity. That said, the state of course has its obligations, and it is important to reinforce that **States have obligations to protect their own populations**.
- **Taxonomy matters** – it is important to be careful to distinguish between the terms "misinformation" (unintentional spreading of false information) and "disinformation" (intentional).
- There may be a need for **new norms**, even if only to **clarify current norms**, which many believe are too vague. That said, it is important to distinguish between norms, which are non-binding, and international law, which is binding.
- It is important to **not focus just on the kinds of attacks that have happened, but also anticipate the kinds of attacks that might happen** – especially in cases where command and control systems of critical infrastructure may be impacted.



Report of October 12, 2021 meeting

Protecting our Economy and Society against Ransomware

Executive summary

Participants agreed that ransomware is in large part a geopolitical issue and requires like-minded governments to work together to eliminate the safe havens cybercriminals are using to escape prosecution. Various diplomatic tools - such as sanctions - could aid this effort, as could existing frameworks of cooperation, such as the Budapest Convention. Relatedly, States should consider their role particularly important given that ransomware may palpably harm people.

Participants agreed that certifying technologies for critically important industries could help, as could regulating cryptocurrency, even if banning it is likely going to be impractical. Emphasizing a multi-stakeholder approach, participants (a) highlighted the importance of vendors, the cybersecurity community, and law enforcement cooperating with each other, and (b) encouraged the development of research in psychology to help design ways to prevent ransomware attacks. Participants stressed the importance of drafting laws in a manner that they are technology neutral and informed by experts with the necessary technical knowledge.

Distilled key recommendations

- Recognizing that ransomware is not just a technical problem but a geopolitical one, the international community of states should work together to **eliminate the safe havens** that cyber criminals are using.
- Various methods in the **diplomatic toolbox** could help eliminate safe havens. These methods include sanctions. Though it can be difficult for countries to coordinate **sanctions**, they should work towards it, as it can be an effective tool.
- Governments looking to work together to address ransomware should consider building on e**xisting frameworks of cooperation**, such as the Budapest Convention, where appropriate. Otherwise, they may seek to reinvent the wheel, which can unnecessarily and substantially delay progress.
- From a technical standpoint, a **certification** system for tools and technologies at least for certain industries, potentially in areas of particularly critical infrastructure, could help advance protections.

- A range of stakeholders should communicate and cooperate with each other to prevent and mitigate the harms of ransomware incidents. These stakeholders include, for example, **vendors**, the **cybersecurity community**, and **law enforcement**. But overall, multistakeholder co-operation remains crucial in this space.
- Experts from the **social sciences**, including experts in **psychology**, should play a substantial role in helping design effective measures to prevent ransomware attacks. The social science research on such measures is currently insufficient.
- Currently individuals with legal and policy backgrounds drive the development of laws and policies related to ransomware – more people with the relevant **technical knowhow** should be part of that process. Relatedly, laws and policies should be drafted in such a drafted in such a manner that they can actually be enforced. Further, these laws and policies should be **technology-neutral**. This is because such laws and policies can take years to negotiate and amend, while technology evolves quickly.
- A question to consider is **how prescriptive** laws, regulations, etc. should be. A gradation of prescriptiveness may be worth considering – i.e., certain areas/sectors may need more prescriptive regulation than others.
- There is currently a significant **shortage of skilled cybersecurity professionals**; stakeholders should work together to **build such capacity**. Relatedly, individual organizations should invest more in cybersecurity; as it stands, many entities still underestimate long-term risks.

Annex B:

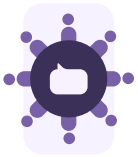
Implementing Cybersecurity Norms on Critical Infrastructure - Perspectives from the Paris Call Community

The work of Paris Call Working Group #4 was supplemented by a community survey conducted by KPMG and Microsoft. The main focus of the survey was to identify some of the key challenges and best practices in implementing Paris Call principle #1 (Critical Infrastructure Protection). Following the survey completion, a dedicated workshop for a European audience was held at the European Cyber Agora conference, where the interlinkages between legislative files such as the NIS Directive and cybersecurity norm discussions were analyzed. The survey was further supplemented through a Paris Call community discussion. The following pages outline highlights from the survey and the related meetings.

Project Design & Key Activities

Online Survey

- Quantitative / multiple-choice survey (with some open questions)
- Questions based on NIS 2.0 & new EU Cybersecurity Strategy (focus on critical infrastructure / Principle 1)
- Target group: all Paris Call signatories (1000+)



Roundtables with different focus groups (e.g. per sector)

- Focus group discussions to obtain qualitative / contextual input to enrich results from the survey
- Target group: selected respondents from the survey / Agora participants

Analysis outcome-oriented discussion on results

- Preparation of initial results based on survey and focus group discussions
- Discussion and funneling of results through working groups
- Target group: Working Group on Advancing International Norms

Report & presentation

- Written report on project activities & results
- Target group: Paris Call signatories, Working Group on Advancing International Norms, other interested parties / public

Overview of activities to date

To gather insights from the Paris Call community, an **online survey** was conducted in May 2021. Following this, a **workshop with small-group discussions** was held to gain further insights, on 3 June 2021, at the European Cyber Agora, which was open to members of the public. On 8 July 2021, the results from the survey and from the Agora focus group discussions were presented to the Working Group on Advancing International Norms.

Survey

A survey to identify good practices and key challenges in implementing Paris Call Principle 1 was launched within the Paris Call community. The survey also aimed to gain insight into the general dynamics of building and implementing cybersecurity norms – e.g. the interaction between public and private sector actors. Although the focus of the survey was on Europe, and most answers came from EU participants, results were also captured from other regions and countries, including Canada, South Africa, UK, and USA.

Dialogue with the Community

Results from the survey were presented and discussed in-depth in focus groups during a workshop at the European Cyber Agora. The key take-aways from each focus group discussion were then shared with and further discussed with all workshop participants (21 participants representing 7 countries and 7 sectors). The results and main take-aways of both the survey and the European Cyber Agora workshop were thereafter shared and discussed with the Working Group on Advancing International Norms.

Results

Survey outcomes

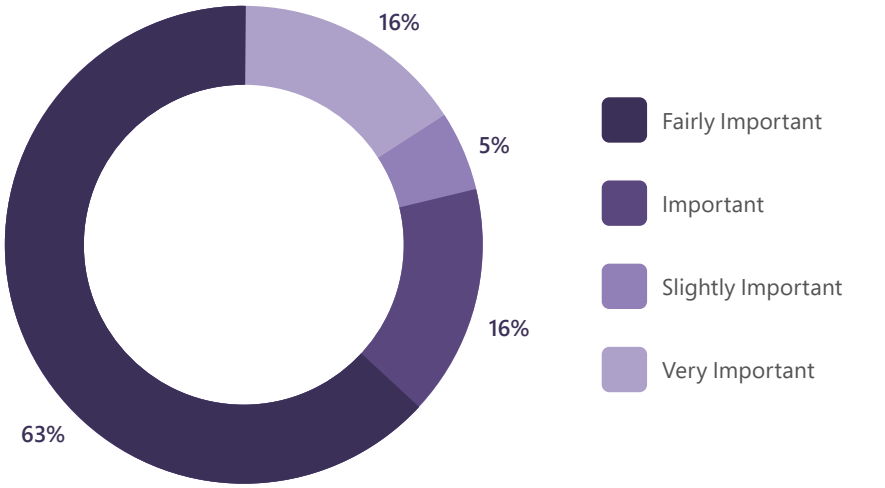
Survey participation and motivation of participants

The survey shared within the Paris Call community was answered mostly by EU participants, but also saw responses from Canada, South Africa, the UK and the USA. Participants included a mix of private (40%), government (20%) and other entities. 80% of respondents reported that they (the entity they represent) are committed to cybersecurity norms due to ethical considerations – and explicitly not for e.g. financial reasons.

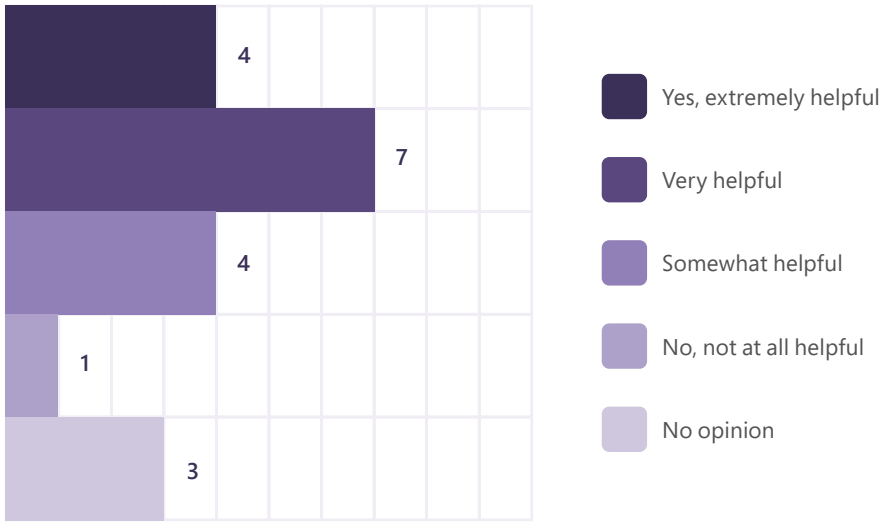
Relevance of cybersecurity norms

Most respondents were not involved in the development of either regional or international cybersecurity norms before signing the Paris Call, but most cited the implementation of cybersecurity norms as an important element in their daily work.

How relevant is the implementation of existing international cyber norms (e.g. the Paris Call Principles) for your entity?



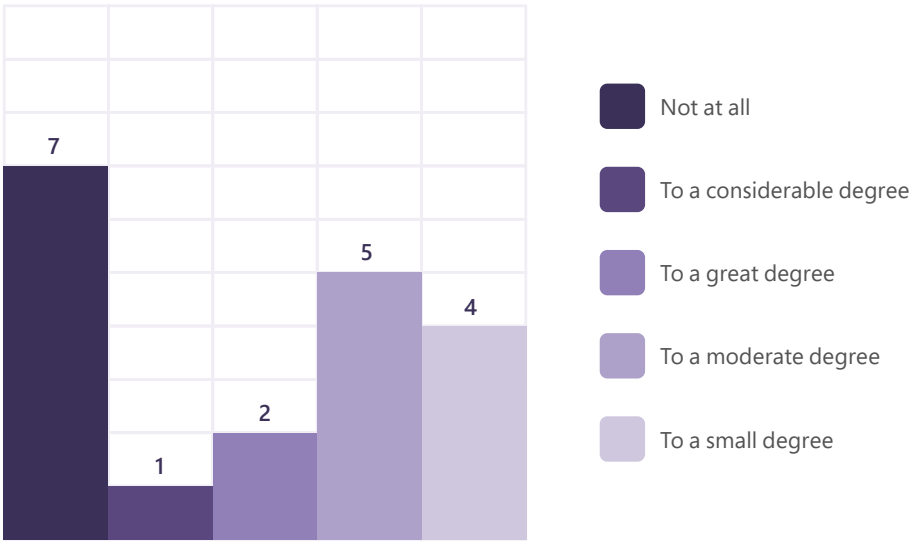
Do you believe that existing international cybersecurity norms help your entity achieve its cybersecurity related goals?



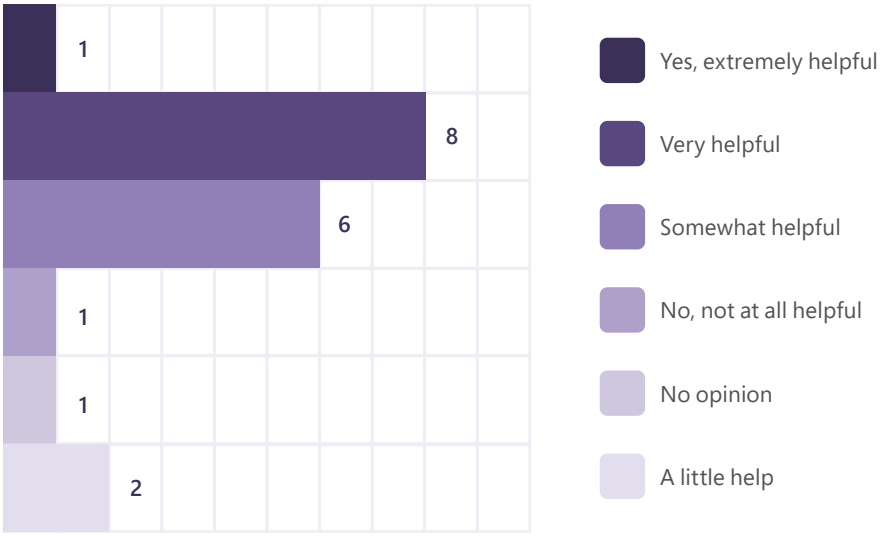
Engagement in the development of cybersecurity norms

Most participants reported that they are involved only to a limited extent in policy discussions at the national and/or international level on critical infrastructure protection (Paris Call Principle 1). However, the dialogue between the public and private sector in general is perceived as beneficial – signaling an opportunity for improving engagement between the different players.

Are you (the entity you represent) actively involved in government-level discussions on how to achieve the goal of Paris Call principle 1 (critical infrastructure protection) in your country?



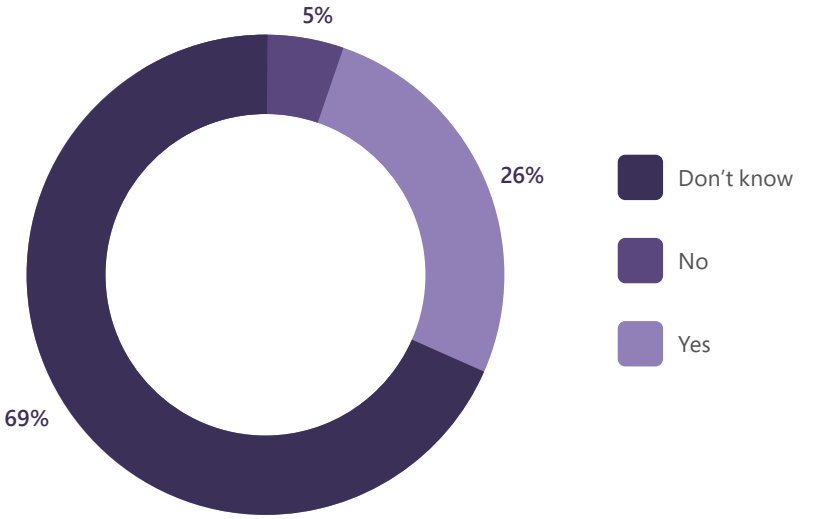
In your country, do you consider the public-private cooperation around critical infrastructure protection to be successful/effective?



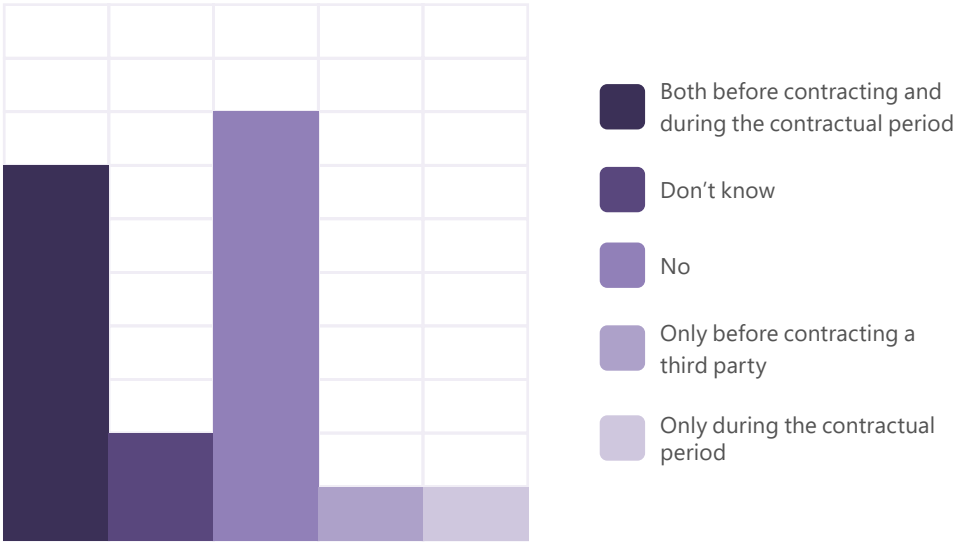
Operational aspects of infrastructure protection (crisis management & supply chain management)

Part of the survey also looked into operational aspects of cybersecurity norms on critical infrastructure protection, using the examples of crisis management as well as supply chain management as important factors for resilience. One third of respondents reported that the entity they represent does not have an incident response plan, and over 40% reported that their entity does not perform any risk assessments on suppliers. This could mean either a lack of prioritisation of such measures, and/or limited awareness.

Has your entity established an incident response plan, crisis management plan or busines continuity plan for major security incidents or crises?



Does your entity perform (cyber) risk assessments on vendors/third parties before engaging with them, and/or during the contractual period?

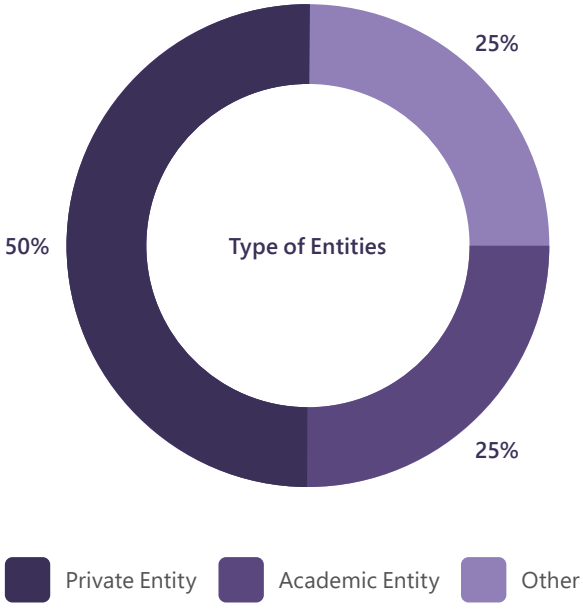


In addition to the aforementioned observations, the survey showed that cooperation between different actors can still be improved. For example, most respondents reported they (the entity they represent) are not involved within Computer Security and Incident Response Team (CSIRT) networks or are a member of Information Sharing and Analysis Centers (ISACs). Further to this, the survey revealed mixed responses on whether or not respondents shared information with other industry stakeholders, and the frequency with which respondents shared information also varies greatly.

Dialogue with the community (results from the European Cyber Agora workshop)

General observations

The results from the survey were subsequently discussed during a workshop at the European Cyber Agora. The following figures illustrate the participant composition of the Agora workshop.



21

Participants

3

Break out rooms

7

Represented countries

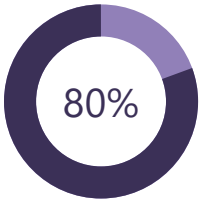
Netherlands, Ireland, USA, South Africa, UK, Belgium, Switzerland

7

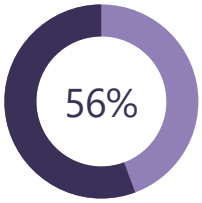
Represented Sectors

Soft-and Hardware, EU Affairs, International Law, Digital, Energy, MedTech, Telecommunications

Questions similar to those in the survey were also asked again during the workshop, diving further into the topic of collaboration.

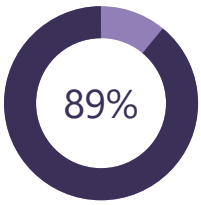


Share good practices/ lessons learned

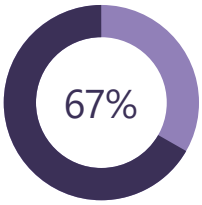


Involved in the development of cyber norms

While 80% of Agora participants share good cybersecurity practices and lessons learned on cybersecurity with other entities in their respective sectors, there was a mixed response on involvement of developing cybersecurity norms at both a national and international level.



Existing cyber norms help achieving goals



Implemented existing international cyber norms

While 89% of respondents believe that implementing existing international cybersecurity norms would help their entity achieve its cybersecurity related goals, only 67% of respondents actually implement these existing norms (e.g. the Paris Call Principles).

Results from the focus group discussions

The Agora was an opportunity for the community to discuss good practices, key challenges and opportunities they see in cybersecurity and developing norms, based on results from the survey. Participants were split into three groups and later exchanged their views with the wider group.

Group 1 Group 1 discussed the strong need for a common understanding of cybersecurity norms and pragmatic approach to turn ideas into practice. The other groups also touched on this topic, adding in the plenary discussion that norms are not perfect, but provide a way for entities to mature.

Group 2 Group 2 talked about the varying perceptions on the importance of cybersecurity across different countries/cultures and sectors and the lack of collaboration between different stakeholders. This group also noted the limited voice of civil society in cybersecurity norm discussions, as this process is perceived by relevant actors as too bureaucratic.

Group 3 Group 3 noted that today's cybersecurity norms are too vague and are not providing sufficient practical guidance, allowing different interpretations to exist. This leads to problems with implementing cybersecurity norms. However, it was also noted that cybersecurity norms in principle are a worthy endeavor.

Below are shown some of the good practices which are applied by the entities represented by the participants of the workshop and the opportunities for the future.

Good Practices

'Could you share with us a cybersecurity good practice that your entity uses?'

- Zero trust model
- Multistakeholder engagement and sharing of information
- Password change, cybersecurity risk register, third parties training
- Cyber crisis simulation
- Risk management for shared responsibility with customers
- Software Bill Of Materials (sBOM)

Opportunities

'In general, where do you see the greatest potential for cybersecurity norm implementation within the sector your entity mostly operates in?'

- Identifying common benefits
- Fostering multistakeholder engagement
- Raising awareness
- Cybersecurity hygiene
- Baseline security
- Transparency and collaboration
- De-escalation of geopolitical tension
- Supply chain security
- Protect personal data
- Standards & certification