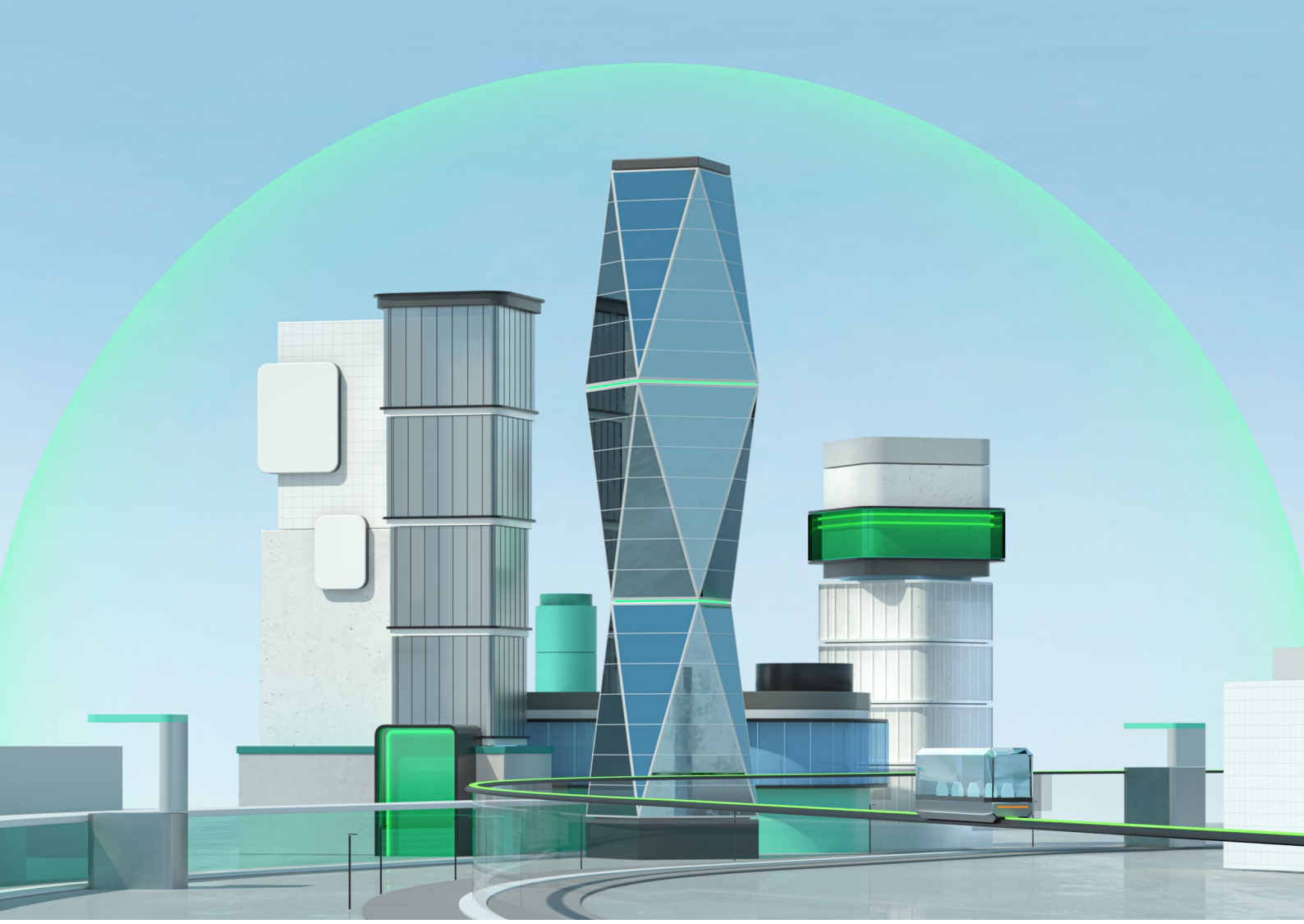


Community talks on cyber diplomacy

Summary of a short series of multi-stakeholder conversations

kaspersky BRING ON THE FUTURE

Learn more on kaspersky.com

Table of contents

What are the Community Talks?

A short series of multi-stakeholder community talks on the global issues organized in late 2020 and early 2021, aimed at identifying, collecting and sharing a number of actionable points from different stakeholders' perspectives on what can help us – the global community – live and prosper in cyberspace.

Another goal was to help the private sector and technical community learn more about the UN cyber-dialogue (the UN OEWG) and how they could support UN Member States in maintaining international security and peace.

After each talk, we now share a summary of the key challenges and necessary actions to be taken as identified by leaders and key experts.

We hope you enjoy!

Are we en route to losing the fight to ensure stability in cyberspace?

#1

Some would say that – yes, finally, this strange year of the 2020 year is nearing its end and hopefully next year will be less stressful for all of us (and we're certainly among those saying it). But still, this year was an important one for those who work to ensure that all things cyber are stable, secure and safe.

Just before the holiday season starts, we gathered for the first in a series of multi-stakeholder Community Talks on Cyber Diplomacy to review 2020 and, particularly, discuss if we as a global community might be heading toward losing the fight against cyberthreats.

Experts:

Camille Morfouace-de Broucker
French diplomat and former policy advisor on Cyber Issues at the Ministry for Europe and Foreign Affairs

Craig Jones
Cybercrime Director, INTERPOL

Pierre Delcher
Senior Security Researcher at the Global Research and Analysis Team (CReAT), Kaspersky

Are we a step closer to reaching stability in cyberspace or not? Should we close the 2020 chapter on a pessimistic or optimistic note? Are we losing or winning the fight to ensure stability in cyberspace?

We gathered cyber diplomats, cybersecurity researchers, the technical community, academia, and law enforcement professionals, who all help fight cyberthreats but from different angles.

We discussed three questions:

- What we do well and what are the best practices;
- Where we failed or are failing; and
- What, accordingly, should the priorities be for further work.

We shared what we know, asked about what we don't know, and talked and discussed to learn from each other as to how to best keep cyberspace a comfortable and secure place for all of us.

So what did we discover in the first Community Talk? Has anything positive happened to us in 2020?

(Note: Though many of us might believe that the year 2020 has been challenging and number of cyberattacks around the world continues to grow, we still witnessed many important achievements at the global level.)

For the first Talk we had the pleasure of having the following experts participate:

- **Camille Morfouace-de Broucker**, French diplomat and former policy advisor on cyber issues at the Ministry for Europe and Foreign Affairs (@CMorfouace);
- **Craig Jones**, Director of Cybercrime, INTERPOL (@INTERPOL_Cyber); and
- **Pierre Delcher**, Senior Security Researcher of the Global Research and Analysis Team (GReAT), Kaspersky (@securechicken).

Starting with the positive reflections (recalling the good things that occurred in cyberspace in 2020), we learned that, from a cyber diplomacy perspective, the global community has progressed in strengthening multi-stakeholder consultations within the UN OEWG, which recently launched its 'LetsTalkCyber' Dialogue Series. **Camille** also noted that France, particularly, decided to take a step further to create a more inclusive and action-orientated framework, with dedicated discussions open to exchanges with other stakeholders to make the UN cyber-stability framework work. Thus, France, as 45 other States proposed to create a Programme of Action under UN auspices.

From a law enforcement angle, **Director Jones** shared that during the pandemic INTERPOL had to swiftly adapt its work to the new environment, since the criminals adapted very quickly to exploit the COVID-19 situation. However, cybercriminals' attacks and methodologies have not changed, while INTERPOL managed to successfully work with national police and 12 private partners for remote cybercrime investigations. The national cybercrime untiscontinue work effectively in the online format. Raising awareness remains important work, and INTERPOL also launched the #WashYourCyberHands campaign to ensure that both individuals and businesses are equipped with the knowledge of how to protect their systems and data.

Finally, **Pierre**, speaking on behalf of the cybersecurity research community, highlighted that in 2020 threat-intelligence researchers managed to successfully discover new attacks and threats, including advanced state-sponsored activities, and the Kaspersky team demonstrated that 2020 threat predictions were accurate: notably, GReAT anticipated an increase of targeted ransomware and geopolitics as the driving force behind APT attacks (btw, check the 2021 threat landscape predictions here). **Pierre** also mentioned that the pandemic hasn't prevented researchers from advancing cybercriminal investigations together, including with the technical community and LEAs (Europol and INTERPOL). In 2020, Kaspersky also joined FIRST to enhance cooperation with the network of CERTs.

Were there failures in our work? And if yes, what are the priorities for 2021?

Despite the achievements, there is still a lot to do to further cyberstability. **Camille** mentioned that capacity building and developing further cyber governance as the 'fruit' of discussions between states and all stakeholders – the key to cyberstability. Multi-stakeholder engagement is essential and this idea is at the heart of the Paris Call, and in 2021 there will be six Working Groups for achieving more practical results. Within the UN, we need to work on national implementation of already agreed 'cyber-norms', and hopefully within the UN we will be able to have an inclusive framework to focus on how countries implement norms and which capacities they might need for that.

Director Jones agreed that the standard-setting process at the UN is critical. INTERPOL wants to protect the community and prevent cybercrime, but doing this job in the global context is still challenging: not all countries have yet prioritized the cybercrime issue and not all countries have legislation covering it; in many cases – roles and responsibilities remain unclear. Therefore, we have different definitions and different understandings of the one and the same problem. Addressing security-by-design in technologies and enhancing trust for building stability are also existing challenges. Quite often, national strategies look great on paper, but in practice there's a lot of work still to do to make them really work, with sufficient resources and sufficient harmonization. Addressing a question from **Dr. Katherine Getao**, CEO of ICT Authority, Kenya, about how police forces should collaborate in a more visible way, INTERPOL will continue building closer networks among national police forces, boosting cooperation with FIRST for an effective cyber global response program, and further establishing partnerships with private actors.

Pierre agreed on closer cooperation, but said that we as a global community are still failing to make cyberspace more stable. Attacks grow, states are rapidly developing military and offensive cyber capabilities with little transparency and this alarming trend might exacerbate the existing risks in cyberspace. Speaking on behalf of cybersecurity researchers, **Pierre** stressed that we need effective global cooperative regulation or control mechanisms to prevent confrontation in cyberspace, and to enhance transparency on the use and development of cyber capabilities.

To a question from **Eric Axel Behrendt, Global Corporate Development Manager, APAC, TÜViT**, asking if a code of conduct for responsible behavior is possible in this regard, **Camille** recalled that this is a separate process within the UN to fighting cyber criminality, and targeted answers should be developed to targeted problems. For a start, we need to ensure that all understand the rules in cyberspace and that there's enough knowledge to check that agreed norms are implemented. That's why France proposed the PoA as a next step forward and a more pragmatic approach.

Blitz poll!

As the main purpose is to learn from each other, we also asked three quick 'blitz poll' questions to the experts:

- **The key event of 2020 that had the greatest impact on the global community?**
  All three experts agreed that it was the pandemic, changing our work and life in general.

- **The key event/process the community needs to follow in 2021?**
  Pierre answered the Security Analyst Summit (SAS); **Camille** mentioned the reports of the UN OEWG (March 2021) and UN GGE (May 2021); while **Director Jones** stressed that the year 2021 will be important for INTERPOL in building a closer and more effective cooperative network among national crime units, private partners, and the technical community.

- **What to read/check for learning more about cyber diplomacy?**
  Books on reverse-engineering are #1 in **Pierre**'s list; **Camille** announced that in 2021 the Paris Call should publish the results of the exchanges of the working groupe; while **Director Jones** stated that INTERPOL's global threat assessment report will be published next year too.

Before you go

Before you go, please check the following useful resources shared at the Talk:

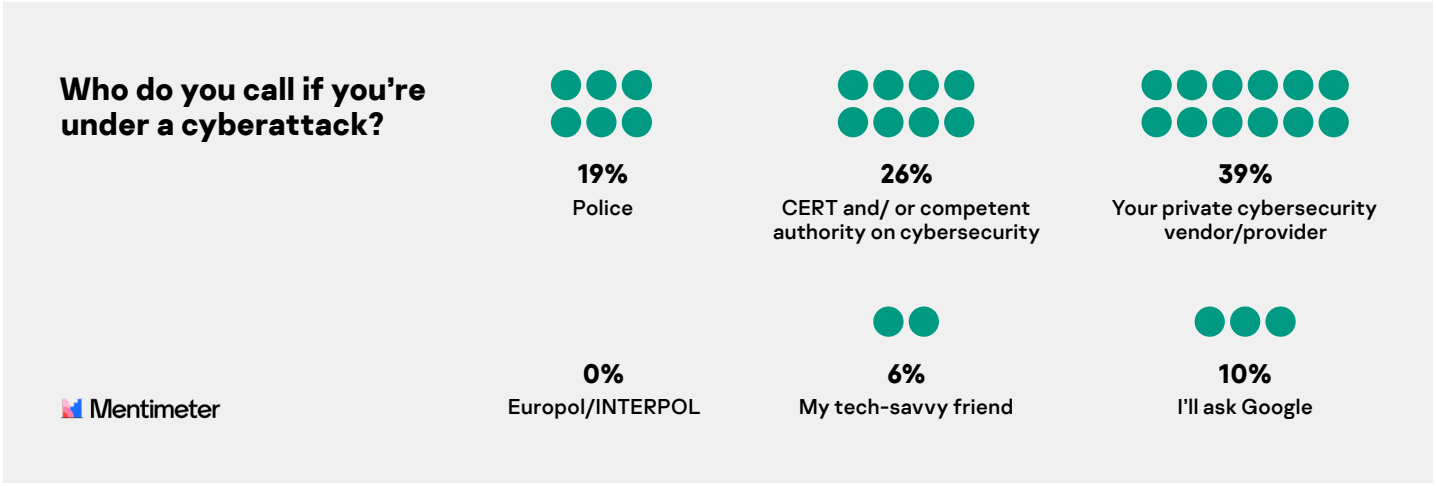
- INTERPOL COVID-19 Cybercrime Analysis Report
- **Pierre**'s article on the Researcher's call for a determined path to cybersecurity
- The Geneva Dialogue on Responsible Behavior in Cyberspace and its 2020 Outcome document on security-by-design
- Kaspersky's submissions to the UN OEWG (March 2020; June 2020; September 2020)
- The IGF Dynamic Coalition on Internet Standards, Security and Safety

You can re-watch the Community Talk here https://kas.pr/g4ss.

Who do you call if you're under a cyberattack?

#2

We organized Community Talk #2 and asked guests to share their answer: 39% said that their private cybersecurity vendor/provider would be the first on the list; CERT and/or a competent authority on cybersecurity comes second (26%); and police comes third (19%). The results you can see below:



Experts:

Ambassador Nadine Olivieri Lozano
Head of International Security Division, Federal Department of Foreign Affairs, Switzerland

Neil Walsh
Chief of Cybercrime, Anti-Money Laundering and Counter Financing of Terrorism Department, UN Office on Drugs and Crime (UNODC)

But that's not all. We had the second edition of our Community Talks on Cyber Diplomacy – no ties, no overly-formal discussions – to hear what cyber diplomats, cybersecurity researchers, academia, policy experts and law enforcement professionals fighting cyber threats also think. This time we had the honor of discussing this topic in greater detail with:

- **Ambassador Nadine Olivieri Lozano**, Head of International Security Division, Federal Department of Foreign Affairs, Switzerland (@SecurityPolCH);
- **Neil Walsh**, Chief of Cybercrime, Anti-Money Laundering and Counter Financing of Terrorism Department, UN Office on Drugs and Crime (UNODC) (@NeilWalsh_UN);
- **Ivan Kwiatkowski**, Senior Security Researcher, the Global Research and Analysis Team (GReAT), Kaspersky (@JusticeRage); and
- **Stefan Soesanto**, Senior Cyber Defense Researcher, CSS/ETH Zurich (@iiyonite @CSS_Zurich) as **discussant** – a special role to challenge the discussion of the three panelists and provide an additional opinion from a researcher policy perspective.

We focused on discussing existing and possible cooperative mechanisms in case of a cyber emergency and cyber incident and, particularly, on the implementation of the existing norms on critical infrastructure protection and assistance[1].

For every Community Talk we discussed three simple questions, and for Community Talk #2 they were as follows:

1. What best practices already exist (and how far we as the global community went in implementing voluntary 2015 UN GGE norms G and H)?

2. What didn't and doesn't work to implement those norms and create effective global response frameworks?

3. What the priorities are for the global community in 2021 in this regard?

Starting with the positive reflections (recalling the existing good practices), **Neil** stressed the global community has norms, but they are beneficial only when they are actually operationalized and used. For implementing norms G and H, one of the first steps should be exploring cross-government culture as well as looking more into what capabilities we see that states have more and more advanced offense and defense cyber capabilities. **Neil** also mentioned that we have to build a government-based response, and within countries we should use all capabilities to try to understand the threat we are facing; otherwise discussing how a response should look without understanding the threat gets us merely into a philosophical debate. Overall, if we understand the threat, then we will be able to understand the areas of consensus among actors, and only then will we be able to move the discussion forward.

[1] Those non-binding norms, as adopted by the UN GGE in 2015, are: (1) 'States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions' (norm G), and (2) 'States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty' (norm H).

Ivan Kwiatkowski
Senior Security Researcher,
the Global Research and Analysis
Team (GReAT), Kaspersky

Stefan Soesanto
Senior Cyber Defense Researcher,
CSS/ETH Zurich

From a cybersecurity research perspective, **Ivan** said that many good practices for protecting CI already exist. They are: (1) making sure that systems are updated in a timely fashion; (2) deploying endpoint protection on the machines; (3) having offline back-ups of critical data; and (4) investing in human resources capable of detecting and reacting to anomalies inside the internal network. Speaking of global cooperative mechanisms – we fortunately have ways to cooperate more actively with CERTs, INTERPOL, Europol, and national cybersecurity agencies; however, there are no truly structured means for more operational cooperation and global responses in case of a cyber emergency affecting several countries and CI. **Ivan** added that he wished the norms were more detailed for more effective action. At the same time, we see at least private companies are more directly involved in global cyber processes cooperating with the public sector, and he expects to see increased threat intelligence sharing, transparent incident response processes and customer identification programs.

Finally from a cyber diplomacy angle we learned from **Ambassador Olivieri** that the matter of national CI protection (CIP), which is discussed within the UN Open-Ended Working Group (OEWG), is a complex question as different countries have different views on it. What's more, CIP is a matter of national prerogatives and responsibility. In Switzerland, the Reporting and Analysis Centre for Information Assurance (MELANI), together with the national Computer Emergency Response Team (GovCERT), are tasked to protect CI by also participating in national and international info-sharing foras.

Nadine also added that the good practice for all states would be ensuring a trusted and efficient flow of information between operators of CI and relevant government actors as ICT threats are dynamic and volatile and need to be addressed in a swift and targetable fashion. With regard to the implementation of norms G and H, we have a mixed picture: as a takeaway from the current UN processes, states are at very different stages. Some have come a long way and have developed internal procedures, and some are just beginning to identify what CI is and develop processes to protect them. Many states are in-between these two extremes, but at the OEWG there are some national degelations that they did not even know those norms had existed before. So what we need is to raise awareness, help countries that are lagging behind, and give guidance on norm implementation in the format of capacity building, inter-state consultations, and multi-stakeholder dialogues. **Nadine** agreed with Ivan that norms are not detailed enough, and that's why what is needed is to work on further implementation guidance rather than creation of new norms.

Where are we failing: what didn't and doesn't work to implement those norms and create global response frameworks?

Neil started and said we currently face the 'policy vs. reality' dilemma: we're hearing from someone like Ivan working in the tech industry that we don't really have specific language in norms, whereas it takes months and years of discussion for diplomats to agree on the language for norms because there are always strong political disagreements among states. Sharing from personal professional experience, **Neil** said that states face the same threats and the same cyber risks, and when Neil and his team, which is located on six continents, speak to states, all agree that we need to build cyber capacities; however, there are many factors – regional, political, legal, etc. – that influence this. We need a private sector whose role is to advise and guide these critical discussions. Yes, it is the decision to be made by states to allow the private sector to be in a room or not, but the risk we all face right now is while decision-makers discuss policies, and the private sector takes proactive steps already – this leads us to a discrepancy and moves us further from the reality, and therefore limits our capabilities to address the threats.

Ivan, sharing the cybersecurity research perspective, agreed with Neil about the gap between intent and implementation, but also mentioned that the norms are only a first step in the right direction, while there are still a number of issues that need to be addressed in the interest of global cyber-stability; namely: (i) acceptable use and regulation of dual-use software, such as commercial Trojans and zero-day exploits; (ii) more transparency regarding the alleged stockpiling practices of software vulnerabilities of national security services; and (iii) the lack of a common framework (or at least shared practices) to attribute cyberattacks. **Ivan** also stressed that while countries share more policies about their cyber engagements, there is, however, no information on how they would react to attacks. In the interest of deterrence, it would make sense to clarify the precise consequences for cyberattacks wherever possible.

Nadine supported both points on the 'policy vs. reality' gap and Ivan's statements on the deterrence and attribution, but also added that when it comes to detailed discussions on CIP – it becomes a very sensitive issue. While the collaboration works quite well between technical specialists and CERTs, the discussions get tricky at the political level as it is becomes difficult to find the right words that everyone would agree to. However, what all states agree within the GGE and OEWG is that capacity

building is crucial, as is building global expertise to have stable structures and frameworks to deal with ICT threats.

Nadine also shared that governments tend to work in silos and there are many people within governments themselves that have not heard of norms too. She mentioned the example of Switzerland: when establishing its national cybersecurity strategy, it has been extremely useful in bringing different actors together to learn about each other's work. So the same is needed at the inter-state level for building capacities and for implementing norms.

Jan Lemnitzer, Cybersecurity policy expert and lecturer at the Department of Digitalization, Copenhagen Business School, and **Vladimir Radunovic, Director of E-Diplomacy and Cybersecurity at DiploFoundation**, posed additional questions on how the response would be if a state does not have capacities to respond to an assistance request (norm H) and on how interaction between the public and private sector and security/tech communities should look.

Addressing them, **Neil** said in both cases that the response would depend on the scale and complexity of the attack. When states don't have capabilities to address a cyber incident or provide assistance, at least they can share what technical information, attack vectors, some ideas of evidence and intelligence they might have. Hence, transparency and the ability to communicate becomes critical, and all types of response would therefore largely depend on relationships among states. **Nadine** added that cross-border cooperation is critical, but it concerns not only governments but private sector too. Speaking of norm H and the 'due diligence' principle, states need to do what is reasonably feasible for those states; i.e., if they don't have the capacity they should reach out to other states, and Switzerland, particularly, has had cases when it helped other countries deal with cyber attacks. Bilateral mechanisms are important, but also the global community has other mechanisms of capacity building, e.g., the Global Forum on Cyber Expertise (GFCE), the World Bank's efforts, the Organization for Security and Co-operation in Europe (OSCE), Organization of American States (OAS), and ASEAN.

To all these thoughts, **Stefan** provided his additional opinion and agreed that info sharing is important, but that states are not always willing to provide assistance to other states. He particularly mentioned the case of how the FBI assisted the Reykjavik Metropolitan police in their investigation of Silkroad - the first big dark web market -, while European law enforcement agencies showed the Icelandic police the cold shoulder. And how NATO has stood up Rapid Reaction Teams since 2011, to support alliance members in the mitigation and triaging of cyber incidents affecting their military networks. However, what is missing in the current conversation, as **Stefan** stressed, is the build-up of deployable national capabilities that can be offered to third states under the umbrella of investigative support, humanitarian aid, or even peacekeeping. Furthermore, **Stefan** noted that governments should ask themselves whether the due diligence principle and state sovereignty should apply to bulletproof hosting servers or whether they should be considered a free game? **Stefan** noted that in the context of Europol's takedown of Emotet, two of the three C2 nodes were most likely hosted by bulletproof hosters. Similarly, the offensive cyber operation that the Australian Signals Directorate ran against foreign criminal infrastructure in April 2020, was most likely also directed against servers at a bulletproof hoster.

When it comes to cooperation among CERTs, **Serge Droz**, **Chair of FIRST**, joined the discussion and said that there is indeed good experience of cooperation among technical specialists and the private sector. The problem arises when politics and policy comes in: particularly, **Serge** mentioned that they are not allowed to exchange technical information with some companies in China. However, while the policy of a particular state might be wrong, it does not mean that we need to allow vulnerabilities to be exploited by malicious actors.

What are the priorities for further work?

Ivan said that his personal priority is to increase the cost of attacks as much as possible (for attackers obviously). **Neil** agreed with that and added that we need greater capacity building and greater investments for cybercrime investigations. **Nadine** supported both points, and added that there is still a lot of work to do to achieve better geopolitics: discussions in the UN are very polarized, but hopefully 2021 will be better in terms of communication among countries.

Blitz poll!

As the main purpose is to learn from each other, we also asked the experts three quick 'blitz poll' questions:

- **The key event/process the community needs to follow in 2021?**
  While **Neil** and **Stefan** agreed that there are many processes in practice to follow, **Nadine** mentioned in particular the cyber processes within the UN First Committee, and **Ivan** mentioned the OFAC's statement that ransomware payments may be in violation of international sanctions.

- **What to read/check for learning more about cyber diplomacy?**
  DiploFoundation's resources and UNIDIR Cyber Portal are #1 on **Nadine**'s list; **Ivan** shared that he prefers anything from Cory Doctorow, Bruce Schneier and Edward Snowden; **Stefan** invited everyone to visit the upcoming conference on cyber sanctions; while **Neil** advised to keep up with what's going on in twitter.

- **Who do you call if you're under a cyberattack?**
  Nadine said that the new national Swiss Center for Cybersecurity would be the first in the contact list; **Neil** was honest that his spouse would be the first he'd reach out to; while **Stefan**, as most of attendees, would call a cybersecurity vendor such as Kaspersky; and **Ivan** would definitely call Costin Raiu first.

You can also re-watch the session here: https://kas.pr/k416

What do we talk about when we discuss "cyber conflict"?

#3

Continuing with the limited series of Community Talks, we organized the third edition to discuss mechanisms for conflict resolution and conflict prevention with the following experts:

Experts:

Sirine Hijal
Deputy Cyber Foreign Policy Coordinator, Global Affairs Canada, Government of Canada

Max Smeets
Senior Researcher, Center for Security Studies (CSS), ETH Zurich, co-founder and director of the European Cyber Conflict Research Initiative (ECCRI.eu)

- **Sirine Hijal**, Deputy Cyber Foreign Policy Coordinator, Global Affairs Canada, Government of Canada (@Sirinaserena);
- **Max Smeets**, Senior Researcher, Center for Security Studies (CSS), ETH Zurich, co-founder and director of the European Cyber Conflict Research Initiative (ECCRI.eu) (@Maxwsmeets);
- **Kurt Baumgartner**, Principal Security Researcher, Global Research & Analysis Team (GReAT), Kaspersky (@k_sec); and
- **Camino Kavanagh**, Visiting Senior Fellow, Department of War Studies, King's College London and non-Resident Scholar, Carnegie Endowment for International Peace (@caminokav), as discussant – a special role to challenge the discussion of three panelists and provide a third-party opinion from a policy researcher perspective.

Each time we discuss three simple questions, and for Community Talk #3 they were follows:

1. What good practices/mechanisms already exist for preventing and resolving conflicts stemming from the use of ICTs/cyberspace?

2. Where have we failed or still are failing: what do we as a global community not have yet for conflict resolution and conflict prevention in cyberspace?

3. What are the priorities for the global community in 2021 in this regard?

Sirine started by emphasizing that most, if not all states are active in cyberspace. This is where geostrategic competition is happening. What matters is what constitutes acceptable or inacceptable behaviour by states in cyberspace. Another level of complexity is that a lot of malicious cyber activity is happening below the threshold of the use of force under international law, that there is a blurring of lines between virtual and physical conflict and a belief by malicious actors that they can act with impunity.

On the positive side, cyberspace is not the Wild West. There is an internationally agreed framework for responsible state behaviour in cyber space, consisting of international law, norms of responsible behaviour, confidence building measures and capacity building. This is, particularly, a key matter for the intergovernmental process in the First Committee of the UN where Sirine leads the Canadian delegation and represents Canada.

Max gave three game metaphors in approaching a definitions of cyber conflict – he sees cyber conflict as a game of poker (signaling game); as a game of chess (advancing without attacking); or as a game of Go (structurally changing the environment to your advantage). Max added that the first type of conflict is the most public one and this is the field where we might have seen already some policy efforts. For instance, the EU Cyber Diplomacy Toolbox is a set of signaling measures of what is acceptable and what is not. The second and third types of cyber conflict are the most important ones, and the U.S. Cyber Command's strategy of persistent engagement is an example that takes the direction of the second type, where the goal is not deterrence, but limiting an opponent's opportunity to act. However, these types requires effort and this is an area where joint strategic efforts between Europe and the U.S. are especially needed.

To this, **Kurt** added that when we discuss 'cyber conflict', we should keep in mind that this usually happens not in an exclusive domain, in a vacuum, and additionally he agreed with the game metaphors by adding that identifying the root cause of cyber conflict often results in a separate discussion of geopolitical games rooted in the various motivations and interests of nations. Sharing also a perspective from cybersecurity research, Kurt said that we have seen large operations, but all of this activity can exhibit marks of espionage, theft on a massive scale, and both destruction and disruption. To be better prepared for conflict resolution and settlement, we need national points of contacts (PoCs) for reporting incident-related data so non-state actors know whom to contact and with whom to cooperate, and ideally these PoCs should be neutral from geostrategic competition/geopolitics to act as firefighters in the event of a significant cyber incident. Cybersecurity researchers, the technical community, and relevant government bodies need to have secure channels of communication, and clear paths to resolution and stability where, again, they can remain neutral as much as possible.

Kurt Baumgartner
Principal Security Researcher,
Global Research & Analysis Team (GReAT),
Kaspersky

Camino Kavanagh
Visiting Senior Fellow, Department of War Studies, King's College London and non-Resident Scholar, Carnegie Endowment for International Peace

Where are we failing: what we as a global community don't have yet for conflict resolution and conflict prevention

Kurt already touched on the gaps and shared examples from his professional experience: in the past, when reaching out to CERTs you generally were met with silence, or they provided notifications for specific devices calling back to a sinkhole, but received no acknowledgement of the notifications; however, often these very specific devices stopped communicating with the sinkholes within 48 hours. Reaching out further and requesting malicious code sharing in order to assist with analysis resulted in silence on the wire as well within 24 hours. Was there more out there to clean up? What happened? There was no data exchanged to further the investigation from the CERTs and the recipient side. We'll probably never know. It's critical that CERTs/CSIRTs can work with non-State actors to gather incident-related information and respond to incidents without interference/pressure to inform political attribution decisions.

To that, **Sirine** noted that we still don't have an agreement among states on the way forward in the normative and legal space. There are also challenges in implementing the existing non-binding norms for responsible state behavior because of different levels of capacities among states and a lack of knowledge about norm implementation. Other states are not respecting their undertakings in this regard. This can sometimes lead to a lack of accountability, i.e., holding malicious actors to account for malicious ICT activities.

In this regard, **Camino** highlighted that,

"**we need to deepen our understanding of how cyber operations figure in armed conflicts, including support or services provided by third parties; how international law, norms and other relevant measures can offer a framework for considering such operations in peace negotiations or settlements; and the range of private actors – technology companies included – with direct or indirect responsibilities in a particular conflict and the degree of responsibility and legitimacy they have in contributing to preventing or resolving a conflict**".

One of the challenges in building accountability in cyberspace is lack of transparency and attribution, as it was correctly highlighted through questions from the audience. Particularly, **Paul Meyer**, **former Canadian Ambassador for Disarmament and currently a Senior Fellow with The Simons Foundation and a Fellow in International Security at Simon Fraser University in Vancouver**, asked how we can assess whether state cyber operations are responsible or not if these operations are conducted covertly. There is transparency in conventional military activity that enables holding states to account; however, this is lacking in militarized cyber activity. **Tyson Johnson**, **Chief Executive Officer, CyberNB CIPnet**, asked where we as the global community go with attribution so there is a way to identify 'ownership' and help ensure we know who the bad actors are. Otherwise, the ability to play poker, chess or Go is limited, as we do not know who we are really playing with. In this regard, the lack of sharing and exchange of technical data is one of the biggest failures in improving defense capabilities and for achieving attribution.

To this, **Kurt** agreed that in a number of instances, the ability for nation states to cooperate among themselves and with non-state actors is too difficult. Harmonizing legal frameworks for mutual legal assistance at the national, regional, and international levels to combat cybercrime and targeted attacks is crucial. We need a shift towards defending better, and on the other hand, we rely on law enforcement to prosecute these criminals. We also need a true coalition to build capacity and to see enforcements of agreements, increased technological cooperation across governments.

Before you go...

Before you go, please check the following useful resources shared at the Talk:

- The European Cyber Conflict Research Initiative (ECCRI) and 'The Big Cyber Ideas Festival' (@BigCyberIdeas)
- Canada's implementation of the 2015 GGE norms and updated norms guidance text
- Canada's commissioned research on gender and cyber (authored by Allison Pytlak and Deborah Brown)
- Brief on 'Digital technologies and civil conflicts' by Camino Kavanagh
- Investigative security reports by Kurt Baumgartner at Securelist.com

How much do we need to know about the cyber threats we're facing? #4

We are all calling for greater transparency about cyber-engagements and greater information sharing, but are there limits to what we can achieve in cyberspace? How much information do we really need? And in the light of the recently adopted final OEWG report, what would the takeaways be for us as a global community?

Experts:

Johanna Weaver
Special Adviser to Australia's Ambassador for Cyber Affairs and Critical Technologies, Australian Department of Foreign Affairs and Trade (DFAT)

Philipp Amann
Head of Strategy of the European Cybercrime Centre (EC3)

Jornt van der Wiel
Security Researcher, Global Research & Analysis Team, Kaspersky

Continuing our limited series of Community Talks, we organized a fourth edition to discuss mechanisms for sharing and exchanging information and determining attribution with the following experts::

- **Johanna Weaver**, Special Adviser to Australia's Ambassador for Cyber Affairs and Critical Technologies, Australian Department of Foreign Affairs and Trade (DFAT) (@_JohannaWeaver);
- **Philipp Amann**, Head of Strategy of the European Cybercrime Centre (EC3), Europol (@fipman);
- **Jornt van der Wiel**, Security Researcher, Global Research & Analysis Team, Kaspersky (@jorntvdw); and
- **Jan Lemnitzer**, JML Cyber Policy Consulting and lecturer at the Department of Digitalization, Copenhagen Business School (@JanLemnitzer), as **discussant**.

For Community Talk #4 the three questions were:

1. What good practices/international mechanisms already exist for sharing and exchanging information and determining attribution?

2. Where have we failed and where are we currently failing: what don't we know as a global community about the threats we're facing in cyberspace?

3. What are the priorities for the global community in 2021 in this regard?

Starting with the positives: what are the existing good practices for sharing and exchanging information between states and non-state actors?

Ms. Johanna Weaver explained that Australia has invested a lot of effort in this field, in particular, by establishing and maintaining the Australian Cyber Security Centre (ACSC), which also cooperates with the private sector and has a trusted info-sharing framework focusing on critical infrastructure protection (CIP) and protection of systems of national importance. Speaking more broadly about incident response, from an operational perspective, the neutral and non-political work of CERTs and, particularly, FIRST is vital in dealing with day-to-day cyber-incidents. At a more strategic level, when dealing with incidents that have the potential to threaten international peace and stability, there are many good examples starting to emerge, e.g., the ASEAN Regional Forum (ARF) has recently established points of contact (PoCs) at technical, operational and diplomatic levels. Knowing who to call is very important during an emergency.

Regarding attribution, **Johanna** highlighted that it's important to be clear about what types of attribution we're talking about. From Australia's perspective, there is: (i) technical or factual attribution (can we attribute this type of activity to a particular actor?); (ii) legal attribution (is there a legal responsibility?) and; (iii) a political decision to respond to the act (this type is often called political attribution). Speaking of good examples, the U.S. has just released a statement attributing the SolarWinds cyberattack to the Russian Intelligence Services, and Australia expressed its support of this statement (as did several other countries).

From a law enforcement perspective, **Mr. Philipp Amann** stressed that law enforcement agencies (LEAs), industry, academia, civil society and the CERTs/CSIRTs community need to work together because they all hold essential pieces of the puzzle that are important for successful cybercrime investigations and to improve cybersecurity in general. However, it has proven to be challenging to put this into practice because of regulatory and legal uncertainties, lack of standards, lack of trust, unclear objectives and requirements and overlapping initiatives, to mention some. One of the examples Philipp shared was from his time with OSCE when the organisation managed to finalize a first set of confidence-building measures (CBMs) – an important step forward, especially from a political perspective. And currently we can see how states use those CBMs in practice to deal with incidents.

Jan Lemnitzer
JML Cyber Policy Consulting and lecturer at the Department of Digitalization, Copenhagen Business School

Speaking of other existing good practices for collaboration and information sharing, the European Union (EU) has the European External Action Service (EEAS) and Cyber Diplomacy Toolbox, as well as the EU NIS Directive (and the current proposal for the NIS 2.0). Within the EU, Europol works closely with ENISA, CERT-EU, the European Defence Agency and other relevant partners; outside the EU, Europol also cooperates with the World Economic Forum (WEF). Industry platforms such as the Cyber Threat Alliance can be named here too. **Philipp** highlighted that Europol is particularly successful at establishing the necessary networks and getting all the relevant participants to the table to support EU Member States in their investigations: e.g., Europol's European Cybercrime Centre's Advisory groups with the participation of industry; cooperation with the CSIRT community and annual workshops with them; and the Joint Cybercrime Action Taskforce (J-CAT) – an operational platform that Europol's EC3 hosts with LEAs of EU member states and other third countries. The J-CAT drives intelligence-led, coordinated action against key cybercrime threats within and outside the EU. Finally, there is the EU Law Enforcement Emergency Response Protocol, which was adopted by the Council of the European Union. As part of the EU Blueprint for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises, it serves as a tool to support the EU law enforcement authorities in providing immediate response to major cross-border cyber-attacks.

Concerning the role and perspective of the private sector and security researchers, **Mr. Jornt van der Wiel** shared that the key starting point is who is running the cybercrime investigation. If it is a state, then, of course, security researchers have to abide by the relevant laws of that state. The challenge is that there are no standard mechanisms for sharing data between the public and private sector, though there are different legal approaches/different state laws on info sharing and info exchange in cybercrime investigations, which security researchers need to keep in mind.

Jornt continued that having transparent communication and managing each other's expectations is critical for effective info-sharing frameworks. The private sector, in particular, often doesn't need private identifiable information – meta data is enough. Companies are, however, interested in meta data and "technical" data that can help them improve cybersecurity detection and response products as well as their investigations into threat actors' campaigns. In summing up, **Jornt** stressed that trusted contacts are key, though things are not so simple when it comes to info sharing, and in many cases trust depends on a particular person and the relationship with that person.

Constructive criticism: what we don't know about the threats we're facing in cyberspace and why

First, **Johanna** stressed that, of course, we need to do a lot more and quickly to address more sophisticated cyberthreats, but we also need to understand that we've come a long way in a short period of time. What's more, our growing ICT inter-dependence creates new opportunities for malicious actors. How do we fix that? Focusing on high-level threats – we certainly won't be able to address them without significantly increasing cyber-hygiene across the globe. The level of maturity in many countries remains low and, for example, some countries are still lacking domestic cybercrime legislation, meaning certain types of malicious activities may not be illegal in some countries. We also need better coordination of incident response (to ensure all countries are equipped to mitigate malicious activity) .

Speaking of state behavior in cyberspace, **Johanna** recalled that the global community, including states, have the UN cyber-stability framework, but we also need to hold the actors accountable. In particular, it's important to be clearer about what the rules are and what happens when those rules are broken. A "global attribution body" is hardly likely to work because the severity of cyber incidents that would be referred to such a body would be inherently connected to national security. States would need to deal with lots of issues on info sharing (as this would require, for example, the sharing of sensitive information related to national security). States are also unlikely to be willing to delegate their sovereign attribution (and response) prerogative to an external body. What we do need though is greater transparency and much clearer expectations of how states should act; this will create greater predictability. Plus, there are many existing tools which we already have and need to make better use of (e.g., referral to the UN Security Council for cyber incidents that have a severe impact).

Philipp agreed and added that from the LEA angle, there are several challenges for investigations and attribution as summarised for instance in the common challenges in combatting cybercrime report which was jointly published by Europol and Eurojust. These include the loss of data, linked for instance to the criminal abuse of encryption, and location; international cooperation and cross-border coordination; public-private partnership. The Crime-as-a-Service (CaaS) model poses another challenge as it provides the tools and services needed to commit cybercrime or cyber attacks.

Speaking of elements for successful info sharing, **Philipp** highlighted that the issue is not necessarily a lack of initiatives and platforms but often overlapping activities or at times the groups can be too big (generally speaking, the more people you have at the table, the more difficult it is to establish trust). More importantly, there is still a lack of common definitions and standaridsation as well as legal uncertainty. There aren't always clear-cut answers to questions like: What kind of data are we sharing? How detailed should the data be? Why are we sharing the information? How long will we store the data? What will happen with the information shared and is it actionable? While we are waiting for the process to emerge [within the Third Committee on developing a legally binding instrument for addressing cybercrime], it is important to use and further promote what we already have – the Budapest Convention in particular. Addressing Johanna's point on cyber-hygiene, **Philipp** agreed that the industry has an important role to play here by ensuring and producing secure-by-design technology.

Another challenge mentioned by **Jornt** is that it's difficult to publish everything the security researchers might want as there are different laws and legal restrictions that need to be considered. Also, it's important to limit the public information so as not to undermine the cybercrime investigation. Speaking of attribution, private companies do the technical attribution, but they do not have the legal capabilities or authority for public or legal attributions that states have. The only thing that companies can do is to tie certain campaigns or malware samples to certain groups, but they cannot tie those groups to individuals.

However, this does not mean that security researchers don't help with investigations. When it comes to attribution, they do the investigation work and based on that, they write a report that can be shared with LEAs. LEAs should then be able to reproduce every step and derive their own conclusion about it.

Our discussant, **Dr. Jan Lemnitzer**, excellently challenged the ongoing discussion. First, he said that transparency in cyber diplomacy is cheap and demands no direct action from states. When it comes to intelligence operations in cyberspace, states will not share that information freely and fully. That's why, in essence, information sharing in cyberspace is about sharing between private industry and regulators or states. For example, the latest FBI internet-crime report reported damages of around $29.1 million caused by ransomware. But we should understand that this is only the data that was reported and shared with the FBI. If anybody ever wants to establish a global figure estimating the true damage caused by ransomware, the real challenge would be finding the information and asking others to share it. **Jan** asked, therefore, to name what really works well in terms of info sharing for addressing ransomware.

Second, he stressed that if we look at existing info-sharing arrangements, trust is key. But when regulators are involved, private actors may behave differently – they will either share not enough (because of the legal risks) or over-report, including on every minor and non-minor cyber-incident, which would diminish the value of the information. Another thing is that many companies expect regulators to share valuable information in return as part of those info-sharing frameworks, but this doesn't always happen.

In response to that, **Johanna** addressed the point on transparency and said that it is indeed vital, but it isn't cheap. For example, Australia is transparent that it has and it uses offensive cyber-capabilities, but, of course, Australia does not disclose details of operations and classified information. However, the fact, that Australia is transparent and publicly commits to use those capabilities in accordance with international law and the agreed norms, is a very important step. Many countries are not being that transparent, nor making such public commitments. And that is concerning.

To a question from the audience on encryption versus cybercrime investigations, **Philipp** stressed that a perfect balance is difficult if not impossible to be found, and that we need to have a more open discussion that involves all stakeholders in order to find an optimal solution without weakening cyber security or encryption in general. **Johanna**, in turn, mentioned the Assistance and Access Act that seeks the right balance and avoids creating systemic vulnerabilities and weaknesses.

Priorities & blitz poll

In response to the question on the key process/event to follow in 2021, **Jornt** said the first priority should be to protect the health care sector and its partners. From a cyber diplomacy point of view, **Johanna** said that the success of the work by the Group of Governmental Experts on cyberspace is a priority as well as Australia's International Cyber and Critical Technology Engagement Strategy. **Philipp** wants the global community to have further success at the UN level, but at the same time to continue using and promoting the existing frameworks, particularly the Budapest Convention, to address cybercrime. **Jan** zoomed in to the EU level and said that the NISD 2.0 as well as success in ensuring cyber supply chain management would be an exciting journey to follow.

What can be read in order to learn more about cyber diplomacy? **Johanna's** top list includes the OEWG website, Carnegie's Norm Index, UNIDIR Cyber Policy Portal, and the GFCE Cybil Portal. **Philipp** recommended checking the OSCE's CBMs, the WEF's website, particularly their initiative on establishing a partnership against cybercrime as well as ENISA's web site and the many relevant technical reports, best practices and assessments they produce. **Jan** voted for the OEWG website too and added the Tallinn Manual 2.0. **Jornt** said that anything interesting that could be useful for LEAs in a cybercrime investigation should be shared with them.

Finally, on the question of who you would call if you're under cyberattack, **Philipp** suggested speaking to your kids first as they could be the source of your IT problem. Though a more serious answer was LEAs, noting that people should not underestimate the help they can get from them and the important role law enforcement plays in combatting cyber threats. **Johanna** also joked that the Russian Ambassador for Cyber Affairs Andrey Krutskikh would be a priority contact because every time something happened to her computer during GGE sessions, Ambassador Krutskikh claimed that "Russian hackers are to be responsible'. In all seriousness though, Johanna said she would definitely call a colleague at ASCS or a large cybersecurity firm. **Jornt** said that he would call his boss – the head of the Global Research and Analysis Team (#GReAT) at Kaspersky, and **Jan** advised everyone to have a printed list of contacts in case of a cyber-emergency, as all digital data would most likely be destroyed first.

You can also re-watch the session here: https://kas.pr/m6bs.

Can we avoid an arms race in cyberspace?

#5

In cyberspace, it is well-known that once a vulnerability is being exploited, many of us will hardly be immune to the risks due to the global nature of technology. There's even a saying that 'if you fire a weapon in cyberspace, it will shoot you back'

Experts:

John Reyels
Head of the Cyber Policy Coordination Staff, Federal Foreign Office, Germany

Kathryn Jones
Head of International Cyber Governance at the UK Foreign, Commonwealth and Development Office

Costin Raiu
Director of the Global Research and Analysis Team (GReAT), Kaspersky

We organized the final – fifth – Community Talk on Cyber Diplomacy, where we discussed the risks of a cyber arms race and use of ICT capabilities for defense and offense, and we zoomed the discussion in to ICT vulnerabilities and what we can do for their responsible treatment to avoid the risks of further malicious use and exploitation. We had the following great experts:

- **John Reyels**, Head of the Cyber Policy Coordination Staff, Federal Foreign Office, Germany (@GermanyDiplo);
- **Kathryn Jones**, Head of International Cyber Governance at the UK Foreign, Commonwealth and Development Office (@FCDOGovUK);
- **Costin Raiu**, Director of the Global Research and Analysis Team (GReAT), Kaspersky (@craiu); and
- **François Delerue**, Research Fellow in Cyberdefense and International Law, IRSEM and a Lecturer at Sciences Po (@francoisdelerue), as **discussant**.

For Community Talk #5 the key questions were:

1. What good practices/mechanisms already exist, between states and non-state actors, for responsible reporting of ICT vulnerabilities and their treatment?

2. Where we failed or are failing: what we as a global community don't have yet for responsible vulnerability treatment to avoid their exploitation?

3. What should the priorities be for the global community in 2021 to enhance transparency in cyberspace about states' and non-state actors' engagements?

Good practices first: what are the existing mechanisms for responsible reporting of ICT vulnerabilities and their treatment?

Starting with a cyber diplomacy angle, **Mr. John Reyels** outlined first successes, which include the recent successful conclusion of the UN Open-Ended Working Group (OEWG) and its consensus report, which re-affirmed many of the previously agreed principles, especially in the current difficult political environment. He also reminded that we are close to the conclusion of the current UN Group of Governmental Experts (GGE)[2], and this month we should expect the launch of the Ad-Hoc Committee negotiating a new convention on cybercrime. Zooming in to responsible reporting of ICT vulnerabilities, we have norm J and confidence-building measure (CBM) C in place, which are applicable at the worldwide level. Additionally, there are regional instruments – particularly within the OSCE, which agreed a list of CBMs and which are already operationalized and used by OSCE Member States. Therefore, the framework has been set up already, and technically it's possible for states to exchange information, including on vulnerabilities. The question isif it is desired politically, and here is where we need to focus.

John also mentioned other mechanisms such as informal exchanges taking place between CERT teams as well as corporate frameworks for exchange of information, given the closer interconnectedness of public and commercial networks. The recent takedown of Emotet malware showed that governments and security forces have the opportunity to act very decisively to terminate ICT vulnerabilities, and this gives us all reasons to be confident about government responses in the future.

Ms. Kathryn Jones also highlighted that we need to look at international and national initiatives first; pooling national initiatives through the international arena is often how states make the progress; therefore, countries can make real progress by just doing things domestically, together with consumers, providers of technology as well as with the IT security community. In the UK, particularly, the National Cyber Security Centre (NCSC) is maturing the national approach to ICT vulnerability disclosure

[2] The UN GGE report has been adopted and published: https://www.un.org/disarmament/group-of-governmental-experts/

François Delerue
Research Fellow in Cyberdefense and International Law, IRSEM and a Lecturer at Sciences Po

and remediation. Specifically, it runs a **vulnerability reporting service** – when someone finds a vulnerability in the UK government online service and can't report to the systems owner, they can report it to the NCSC directly. For the triage phase, the NCSC also provides a summary to the systems owner with a full description of the vulnerability as well as recommendations on how to mitigate it. The UK also has a **vulnerability co-ordination pilot**, which helps improve the UK government's ability to adopt best practices by creating vulnerability disclosure programs for any department. The development of the NHS Covid-19 tracking system and **contribution** by the security community in finding vulnerabilities in this system is an excellent example of a nationwide vulnerability management program. Finally, the **vulnerability disclosure toolkit**, a free online resource that helps implement steps in the disclosure process for public and private actors, can be named as another good practice implemented nationally.

Internationally there is also good news. **Kathryn** highlighted that norm J is the least contentious norm that the GGE came up with in 2015, and this signals that all states have a consensus that this is important. We also gladly see states and other communities taking considerable steps to implement this norm. Mr. Reyels mentioned the OSCE framework, but there is also the ongoing work on norm implementation in ASEAN countries. To learn more about the good practices and progress made at the state level, Kathryn recommended two upcoming documents: (1) the GGE report, which will touch on norms in greater detail; and (2) the **GFCE** norms implementation guide, which will provide examples of how states implement existing norms.

From the perspective of the security research community, **Mr. Costin Raiu** started with an optimistic note sharing that the industry has been doing a lot better than it did 20 years ago, and through continued efforts we are maturing in coordinated vulnerability disclosure (CVD), vulnerability management, and bug bounty programs. Kaspersky, in this regard, has a special/unique position and works in this field from three different directions. First, Kaspersky's dedicated teams work on keeping the software the company uses updated. Second, Kaspersky is, at the same time, a software producer itself and it's also important to make sure that the company's products are not vulnerable. And finally a third direction: his team is looking for vulnerabilities in other companies' software. In this regard, the **Kaspersky Ethical Principles** reveal the company's approach where rule #1 is that all vulnerabilities discovered are immediately reported to the vendor, and all bug bounty rewards are paid. This year Costin's team reported three critical vulnerabilities in one very popular software program. These types of vulnerabilities that they discover are usually attractive to sophisticated threat actors.

Costin also highlighted the development of specialized teams focusing on increasing the security of software (e.g., the **Zero Project**), and the **Microsoft MAPP program**, which facilitates the sharing of vulnerability information between vendors. Concluding, he stressed that the reality is that pretty much every piece of software has vulnerabilities, but what's more important is the speed at which these vulnerabilities are being remediated. So it is not only important to produce secure code, but also to be able to patch holes in it.

Constructive criticism: what we as a global community don't have yet for responsible vulnerability treatment to avoid their being exploited

John pointed out the current implementation gap and added that we're lacking the information on how existing norms are implemented. We are also missing sufficient common understanding of how norms should be implemented, and for that we need further guidelines to make sure we implement these norms in a more uniform way to come up with an effective response. The future **Program of Action (PoA)** might help here, but it would most likely be hard to agree on uniform reporting because it's sensitive. Being more realistic, however, states, at least, may agree on doing the outmost for ICT vulnerability reporting at the national level, and this is already may be a step forward. He also added that we need to keep in mind that some regional organizations haven't identified yet CBMs, and some of them haven't been able yet to agree on the common frameworks, so there's a plenty of work to do in the future.

From a security research perspective, **Costin** continued on existing challenges and, first, mentioned the need to incentivize security researchers to check software further and report it responsible. The issue is that they are sometimes hindered by legal issues – when researchers are threatened legally simply because there is a lack of standardized way of doing security research and reporting its findings. Further, **Costin** mentioned the problem of two polarized worlds: imagine a security researcher finds a vulnerability in a popular browser, and he or she has two choices – either report it to the vendor and get two or 20k US dollars, or go to the market where a vulnerability may be priced at a million dollars (and with the risk of being weaponized further). He continued that we are being told that intelligence agencies need ICT vulnerabilities for

catching criminals; however, he mentioned an interesting case of how the Belgian police recently seized nearly two billion dollars in cocaine after gaining access to encrypted phone network of cybercriminals without weakening encryption or exploiting vulnerabilities. On a final point in this section, **Costin** said that though financial reward is one of the main incentives, if we have more developed and stable programs to incentivize researchers in a safe way – from a legal standpoint – then we might all be able to reach better results.

Kathryn agreed with both John and Costin, and added that the recent UN OEWG report makes clear that capacity building is the key (both sharing the experience and pooling necessary resources), and capacities of states to prevent and respond to are important to consider here, particularly in the context of critical infrastructure protection, and, sure, we need to do more. Also speaking of failures in the bigger picture, we need an open transparent debate on what we want to achieve. States will always look for ways to pursue a strategic advantage, and this would increase competition between them. So we can encourage transparency and standardized handling and disclosure of vulnerabilities (such as the Vulnerability Equities Process (VEP) of GCHQ), but as Costin said there will always be a market for these vulnerabilities. **Kathryn** added that both patching and disclosure are fundamental, but we can't win this patching race. So, a failure here would lie in a lack of our common ability to address security at the very start. We need to work on a new model for cyberspace where stakeholders lead on innovation and development of modern standardization by collaborating across borders, while states traditionally struggle to do so at the same pace.

Dr. François Delerue intervened as a discussant and first agreed on the issue of standardization in this context as well as on the issue to provide greater protection for security researchers. However, in the context of the UN-led discussions, and looking at past examples (EternalBlue, WannaCry, NotPetya, etc.), he stressed that we see that one state allegedly identified a vulnerability and decided to keep it to develop an exploit, and then it was leaked to other actors who re-produced this to target others. So, the question is what responsibility might be for the first actor who decided to keep the vulnerability secret? **François** suggested that, building on norm J, we should be less naïve about a possible general ban on the use of vulnerabilities and their exploitation. Instead we need a more realistic approach by putting off-limits specific types of software (e.g., medical software or software used in critical infrastructure) to make sure that when the vulnerability is identified in such a software, the rule should be that it cannot be used for a strategic advantage and it should be disclosed.

Priorities & blitz poll

To a question on what the key priorities for the global community should be in light of the discussion, **John** named the conclusion of the GGE (and defending the 2015 GGE report's substance in these difficult political circumstances) and potential of the PoA, which could be instrumental to close an implementation gap in developing actionable advice and recommendations for cyber-stability. He added that the PoA for small arms and light weapons can serve as a blueprint for achieving success.

For **Kathryn**, the real priority would be to have real open discussions between states and wider communities (within the PoA) based on greater realism on what states will and won't do as well as on greater technical understanding of the issues discussed (in this regard, publishing states' views on how international law applies to cyberspace is important). We also need a further alignment of conceptual understanding across communities, including the public and media, on what we're talking about (e.g., what constitutes a cyberattack?) to have a more nuanced, transparent, and evidence-based dialogue.

Reflecting on François's remarks on responsibility, **Kathryn** added that indeed most states are building ICT capabilities, and certainly there is room for further discussions on legal and political responsibility once ICT vulnerabilities are retained. What's important is to be transparent however on the use of those ICT capabilities, and few states are transparent about this. The UK has recently published its review where it sets out the vision in the context of rapid technological change, which is re-shaping our societies. This document states that the UK will take advantage of these ICT opportunities which the national cyber force can gain through cyber operations to protect the nation from modern threats in the online and real world. But in doing so, the UK is also taking a progressive and proactive approach by shaping the frameworks that govern cyberspace, upholding existing rules, and building consensus around positive norms of behavior. So, the UK will be shaping international rules and standards in line with the fact that it is using ICT military capabilities.

Costin was also realistic (and less optimistic) that we can't really avoid an arms race in cyberspace as it's already happening, and the speed is probably increasing. More and more threat actors continue leveraging stockpiled vulnerabilities, and we will probably not be able to avoid it. Instead, we should admit it and ask for greater transparency and accountability: transparency on how many vulnerabilities are being traded, acquired, leveraged, and for what particular purpose; and accountability on providing guidelines to identify who is responsible for vulnerabilities leading to large outbreaks that were kept secret and then exploited.

In this regard, **François** noted that we need to continue discussing implementation of the norms, but we also need to move from more general discussions to more concrete questions, including the particular practice and experience. As John and Kathryn previously mentioned, the PoA could be a positive evolution in the UN-led discussion.

In response to the question on the key process/event to follow in 2021, **Kathryn** answered the organizational session of the upcoming new UN OEWG, which kicked off on June 1, 2021, and recommended following this process to see how much stakeholders can contribute to the future process. **Costin** named responsible disclosure and further efforts in this regard. Both **John** and **François** named the PoA as the key process to monitor.

What can be read in order to learn more about cyber diplomacy? Kathryn recommended checking the ASPI's resources on the UN cyber-stability framework. **John** advised to check the work of the IFSH at the University of Hamburg. **François** mentioned the Directions Blog, and **Costin** quoted the 'Holographic Universe' by Leonard Susskind, which suggests the idea that the universe we live in is actually a projection of a two-dimensional world, and this could be applied to cyber diplomacy and cyberspace.

Finally, on the question of who you would call if you're under cyberattack, **François** said a local authority is the best to call as they are in charge in going into a victim's network system. **Kathryn** agreed, and said that, as a cyber diplomat, she would call her lawyer with international legal expertise to establish if there is a breach of states' legal obligations. **John's** number one contact would be the Federal Office for Information Security, BSI, which as he said, has been successful in keeping German citizens safe so far. And if **Costin** faces a cyberattack, he would call first a pizza take-away, as it would be, most likely, a long night .

The limited series of Community Talks on Cyber Diplomacy has been finalized. But we've already heard wishes in the communityto continue this format, and, who knows, maybe we'll come back with Season 2 .

You can also re-watch the session here: https://kas.pr/cej7

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com/

kaspersky.com

kaspersky BRING ON THE FUTURE