Tomorrow's Silver Lining:
Cyber Resilience, Cyber Defence, and New Technologies

Brussels, Belgium | October 28, 2022

Public Report Draft

By Raluca Csernatoni, Kathryn H. Floyd, Patryk Pawlak, and Piret Pernik

"Tomorrow's Silver Lining: Cyber Resilience, Cyber Defence, and New Technologies" was held in Brussels on 28 October 2022. The event was strategically positioned between the NATO Edge Conference and the European Union Presidency's Cyber Conference, creating a public bridge between the two. Funded under a generous grant by the U.S. Mission to NATO, this conference was a partnership between William & Mary, the NATO Cooperative Cyber Defence Centre of Excellence, King's College London, and the EU Cyber Diplomacy Initiative – EU Cyber Direct.

Introductory and Welcome Remarks [Live-Streamed]

Dr Kathryn H. Floyd, Director of the Whole of Government Center of Excellence at William & Mary, opened the event with a call to bring together bright and enthusiastic minds, whether 18 or 88, to dissect and tackle the good and problematic challenges in order to make NATO and European Union member nations more secure and resilient against cyber threats.

Dr Teresa Longo, Senior International Officer, William & Mary, delivered introductory remarks and issued the charge to cultivate and build resilience so that nations may prevent, absorb, or recover quickly from malicious cyber activities.

Next, Mr Richard Holtzapple, Deputy Permanent Representative and Deputy Chief of Mission of the U.S. Mission to NATO, gave the Welcome Address. Calling for fresh approaches, Mr. Holtzapple reinforced NATO's three core tasks: deterrence and defence, crisis prevention, and management cooperative security. All of these align to ensure the key purpose: collective defence to adapt to future, and indeed present, threats. "As we face these ever present and growing threats, we must ensure we are prepared to deter such activities, defend against them, and, when necessary, respond appropriately and with unity," shared Holtzapple. He went on to call for the modernization of the Alliance to meet these cyber challenges: "we are expediting our digital transformation to adapt the NATO command structure for the information age and to enhance our cyber defences, networks, and infrastructure." Holtzapple then emphasized how the NATO nations are "promoting innovation and increasing our investments in emerging and disruptive technologies to retain our interoperability and military edge." "Big data, artificial intelligence, autonomous systems, and quantum computing are changing the world and the way NATO operates," as both sources of risks and opportunities for member nations and allies, said Holtzapple. To be ready, Holtzapple extolled the values of the public and private sectors, academia, and civil society working together to develop and adopt new technologies, establish international principles of responsible use, and maintain NATO's technological edge, like with the Defence Innovation Accelerator for the North Atlantic (DIANA). Mr Holtzapple closed by emphasizing how NATO can prepare for and respond to hybrid activities, while looking to the future.

Panel: "Crossing the Rubicon: When A Cyber Conflict Becomes A (Cyber) War [Live-Streamed]

"Crossing the Rubicon: When A Cyber Conflict Becomes A (Cyber) War" then took the stage. Featured on the panel were:

- Dr Joseph Devanny, Lecturer in War Studies and Deputy Director of the Centre for Defence Studies, King's College London
- Mr Christian-Marc Lifländer, Head of the Cyber and Hybrid Policy Section (CHP), NATO
- Dr Monica Kaminska, Assistant Professor, Institute of Security and Global Affairs, Leiden University
- Mr Oleksandr Potii, Deputy Chairman, State Service of Special Communications and Information Protection of Ukraine
- Ms Andrea G. Rodríguez, Lead Digital Policy Analyst, European Policy Centre [Moderator]

Rodríguez opened the panel reflecting on the past conversations on cyber security and emphasizing that definitions matter, as those help create limits, inform policy, and set the agenda for which priorities to address, with whom, and under what terms.

Potii gave an overview on what is happening in Ukraine with respect to cyber, and the border between cyber conflict and cyber war. With many cyber attacks every day, cities and public services are interrupted. In Potii's opinion, the difference between cyber conflict and cyber war is when "the goal of cyber attacks become not material and financial goals, but social and political goals to destabilize the situation in countries and regions." The political goals could be the disruption of local and national elections, while the social goals could be the creation of tensions. When hackers work toward political goals as often paid by the government, that is cyber war. When a government violates the publicly accepted norms - confidence building measures - in their behaviour in cyberspace, that is also cyber war.

Lifländer stressed the importance of starting with *how* to think about cyber, which will be important if one wants to do something about cyber, and the dichotomy between war and peace. "The closest that we have come to cyber war is strategic competition, where nations seek to gain an advantage…[with] profound implications for your capability development, for the kind of infrastructure structure you need, for the kind of training and education your people need," he emphasized. With respect to what is then done about it, Lifländer highlighted Ukraine to show "it is possible to defend one's self against an adversary as capable as the Russian Federation…the defender also has a role to play." Resilience is important because a nation cannot "defend everything, everywhere, all of the time," but you should be able to "suffer the blow and get back to action as quickly as possible," said Lifländer. Lifländer closed with a discussion on the relationship with industry and the need to get out of one's comfort zone: "we need to think through how we collaborate with industry…we will not be able to get it right without getting the modalities of the collaboration with industry right."

Kaminska built on the Ukraine situation, "successful cyber defence is possible." Continuing, "cyber capabilities are not all that useful tactically in war. Cyber Operations are more useful below that threshold of war for influencing political rather than military outcomes. The term strategic competition is particularly useful," said Kaminska. Addressing the intentional psychological goals of cyber operations to create confusion, Kaminska warned how: "western governments find this a challenge to deal with. They try to assess the intent of these operations. that's not always clear and then the responses to that are not always clear."

Devanny suggested that "the point isn't simply to understand conflict and competition in cyberspace, it's to use that understanding to shape what happens next." "There is a danger of the hyperbole - cyber armageddon, a hacking apocalypse, a digital Pearl Harbor…fixating on the catastrophic scenarios can undermine the extent to which you appreciate or recognize the debilitation effects, that the persistence of much lower level operations can have. The relationship between hyperbole and reality is something that is worth emphasizing or underlining. Improving EU cyber security, improving resilience, makes it harder for your adversaries to compete and to use cyber operations in conflict with you. It's worth thinking about security and resilience alongside competition and conflict…and cyber diplomacy." Devanny posited that "cyber diplomacy

is arguably more difficult than it has ever been, but it's also more important–even more important–than it has been." Devanny then encouraged states to work together to identify and find those norms of responsible behaviour in cyberspace, while warning of the "dilemma of calibrating the effects of your operations," including unintended, systemic, and second-order consequences of state-sponsored operations. Devanny closed by offering a conversation on what the building blocks of a responsible cyber power should be, recognizing systemic effects, consistency, and good faith.

Bringing together the various points made by the panel, Rodriguez summarized "cyberspace is an asymmetric domain in which capacities and capabilities play a role…what we are seeing is precisely this preparation and the work you do behind doors to ensure resilience."

Rodríguez then asked the panel to address: "what can we do when it comes to international collaboration and cooperation? What can we learn from these lessons?"

Potii calls for a House of Cyber Resilience with a cyber culture ecosystem: "we need to build a really good cyber resilience civilian sector, cyber resilient private sector, and cyber resilient government sector." Kaminska added: "the biggest lesson from this [Ukraine] war…is the power of information share and targeted intelligence disclosure. That's been the real edge here." Lifländer cautioned: "we need to get out of this ad-hockery. Collaboration is possible, partnerships are possible. We need to think it through. Everything we do left of the bang needs to become better. Going back to the strategic competition piece and how this domain is used, we need to do it all of the time. If cyberspace is always on, our collaboration needs to be always on." "The key thing going forward…is the verb shaping. Shaping needs to take place at many different levels, including the political level, but also at the technical level with standards," said Lifländer. He emphasized that NATO is "a bit late to the game - we need to think 10 to 20 years ahead about what kind of technology, products we want" and what incentives this provides to industry with the purchasing power of government. Devanny referenced the past: "we have learned that defenders are not defenceless, especially when they have very active partners." He added that, "achieving effects in cyberspace is hard, it is difficult to coordinate delivering effects in cyber and non-cyber operations that are aligned. There are often better ways at achieving effects than cyber operations." Looking at finite resources, Devanny touched upon the hard decisions being made about investments in cyber: "you can't cyber your way across a river, but cyber is important and will be increasingly important."

During the Q&A, Nikolas Ott, Microsoft, posed a question to the panel about mindsets vs. reality: "how much are we getting this narrative across to the ones who reconsider how we approach this environment?" Lifländer was reflective: "our thinking evolves together with the domain…there is hesitancy in coming up with the answer, with the silver bullet that we have it now." Kaminska gave encouraging data: "these concepts are filtering through…these concepts are used, it is generally accepted. The reaction you get 'this is obvious - below the threshold of war is where cyber matters most at the most basic level.' There is that shared understanding." Devanny touched on the role of academics in trying to achieve public policy impacts, while "on the practitioner side, the conversation about cyber strategy is a lot richer. There is a lot more of it than there was ten years ago." Potii explored the motivation driving hackers, the stealing of personal information, and government attacks, as well as how to prevent this motivation through sanctions and other measures. Those in attendance then transitioned into their Break-Out Groups.

Break-Out Groups

Break-Out Group #1: "Cyber Resilience and Cyber Defence" featured:

- Ms Sally Daultrey, Intelligence Analyst, Seven Signals Ltd
- Mr Nigel Inkster, Senior Adviser for Cyber Security and China, The International Institute for Strategic Studies
- Ms Piret Pernik, Cybersecurity Researcher, NATO Cooperative Cyber Defence Centre of Excellence [Moderator]
- Mr Kaan Sahin, Cyber and Hybrid Policy Officer, NATO
- Dr Max Smeets, Senior Researcher, Center for Security Studies (CSS), ETH Zurich; Director of the European Cyber Conflict Research Initiative

This rich discussion centred on the development of military cyber capabilities by different European Union and NATO states, with a question of how to understand the implications of that development. One paradigm presented was: to what extent does this reflect the militarization of cyberspace or are there better ways of thinking about it? Participants had varying thoughts about how much progress had been made in developing military cyber capabilities in member states, and the limits of that developmental process over the last ten to twenty years. The group then discussed the concept of military cyber from China's perspective, with a reflection on the limits of what is known, the development of those capabilities, and how those would be used. This was situated in the urgent strategic context of Taiwan in the shorter or medium term. China, and also Russia, are investing in military cyber capabilities, and have offensive cyber programs across the board.

Rather than exclusively focusing on offensive cyber capabilities, operational activities in the theater, or information and intelligence sharing, Break-Out Group #1 went deep on non-military activities including shaping the space through other means, such as regulations, international law, cyber norms, and standards. As an alliance of democratic nations, NATO is more limited in terms of the mandate, decision making speed, and authority, as well as willingness to escalate. Building on this, the group aimed to develop a shared understanding and clarify what is meant when the concepts or categories of cyber resilience and defence are mentioned. While a literal shared language is not needed, progress in these areas will be eased if experts have a shared set of concepts and an understanding, so they are not talking across each other in policy or academic circles. One idea was to think through more thoroughly what shaping means and how that can be achieved in cooperation with the private sector. A big challenge is to get the private sector on board with collective cyber security efforts, understand what their exact roles and responsibilities are in this area, and to incentivize them to take actions for their own resilience, while also protecting democratic values and freedoms. When discussing the private sector, nations need to evaluate the different response options to malicious cyber activities, and the imposition of costs so that they are meaningful, as technical attribution and the releasing of intelligence inherently entails vulnerabilities for cooperative corporations in addition to the vulnerabilities being opened for adversaries. They analysed different ways of conceiving what the private sector could and should be doing and what the relationship should and should not be between government and the private sector in cyberspace.

The group discussed the pros and cons of being a big and small nation when developing a robust cybersecurity knowledge ecosystem. Being a small country can make building and accessing those pockets of knowledge easier, whereas larger or hierarchical nations can have difficulties finding and using such information.

Participants transitioned to strategic competition and thinking about strategic competition in cyberspace, including with overlap:

1. How to embed values in technologies, and the competition to embed different sets of values
2. Stratum of economic competition
3. Political-military competition

They addressed the extent to which cyberspace is seen as a zone of strategic competition, considering it is a rich and varied global system with lots of interaction, to include social and economic interaction. The group largely agreed that the processes

to discuss and deliberate about the future of cyberspace should not just be multilateral in nature, but multistakeholder with states, civil society, and the private sector each having different roles to play. To tackle how difficult it is to coordinate among various stakeholders, participants emphasized a need to focus on different relationships between technologies, politics, and the role of the military as an institutional actor, balancing these three to optimal effect. Toward the end, a nature bridge emerged as this group also touched up on emerging technologies and cyberspace, and the extent to which these conversations are traditionally siloed and they should not be, as there is important overlap. The idea was presented that nations need a way to assess the net effect, a robust totality judgment, of Artificial Intelligence on competition in cyberspace.

In closing, Break-Out Group #1 stood on three pillars: what are the requirements for NATO strategic effects, what are the solutions, and what are the tools and political will to implement.

Break-Out Group #2: "Cyber Security and New Technologies / Emerging Disruptive Technologies (EDTs)" featured:

- Dr Raluca Csernatoni, Fellow, Carnegie Europe [Moderator]
- Dr Amy Ertan, Cyber and Hybrid Policy Section (CHP), Emerging Security Challenges Division (ESC), NATO
- Dr Lucas Kello, Associate Professor of International Relations, Oxford University
- Ms Zoe Stanley-Lockman, Innovation Officer, Innovation Unit, Emerging Security Challenges Division, NATO
- Dr Bruno Volckaert, Professor, IDLab, Ghent University

The aim of this session was to reflect on how emerging and disruptive technologies or EDTs have become a 'battlefield' for values, economic statecraft, political influence, and (cyber) security and defense concerns. In this respect, the speakers addressed three broad questions:

1. How can we define dual-use EDTs and in what ways are their applications impacting (cyber) security and defence? For instance, how are AI systems and quantum-enabled technologies disrupting (cyber) security and defence?
2. Given that a lot of innovation originates in the commercial sector, how should the inclusion of private actors be mainstreamed into (cyber) security and defense markets and supply chains?
3. What are the ethical, "human-machine" teaming, and oversight considerations of deploying complex EDTs in (cyber) security and defense, especially regarding their effective and responsible governance?

Indeed, the speakers agreed that emerging and disruptive technologies (EDTs) present both risks and opportunities. Greater reliance on EDTs will likely involve growing uncertainty and complexity from the "boardroom" to the "battlefield." In this respect, the panel explored the difficulties that stem from the contested definition of EDTs, their dual-use nature, and ethical considerations. Their uncertain roles as force enablers in future security and defense applications may impact cybersecurity and cyber defense in multiple ways. Accordingly, EDTs do not exist in a vacuum - they are neighbors. International organizations such as NATO and Allies need to understand the full spectrum of implications: from definitional and legal considerations, the fusion of EDTs such as Artificial Intelligence, quantum-enabled systems, data, critical infrastructures, and cybersecurity, to a better situational awareness of their disruptive impact on national security. The panel also noted that because EDTs are still evolving and in their early days of development, various actors need to improve their understanding of which technologies to prioritize and which would be useful for offense and defense operations. Part of this can be harnessing technologies in the right ways, to include strategic competition. Better cooperation between NATO and the EU was emphasized, by finding the right synergies across dual-use research, innovation and development programmes, such as NATO's DIANA and Innovation Fund and the EU's Horizon Europe and European Defence Fund.

In particular, the discussion highlighted how an unclear and contested conceptual understanding of dual-use EDTs may lead to inconsistent approaches to human oversight, strategic planning, situational awareness, foresight, and procurement. Part of this may involve societal questions about the role of government and the amount of trust required. Civil-military synergies and human-machine teaming were two of the main issues flagged by the panel participants. Given that a lot of innovation originates in the commercial sector, specifically in start-ups and small and medium-sized enterprises (SMEs), the inclusion of these actors into the cybersecurity and defense markets and supply chains will be important going forward. Importantly, the panel engaged with the notion of the "sovereignty gap," stressing the fact that governments are increasingly relying on the products and expertise of the private sector, thus outsourcing critical services to the corporate sector with regard to critical infrastructure protections, cybersecurity, and the broader deployment of digital technologies. The dependence is as simple as voting machines and the sanctity of election voting, as well. There is an absence of coherent strategy at national level for designating which technological domain is strategic, where further investments or foreign investment screening are needed. Related to this, the example of China's 5G capabilities was mentioned. Conversely, technological giants are increasingly starting to play a geopolitical role on the global stage, by providing critical services and products, as the war in Ukraine has shown.

NATO needs to look at how to foster better adoption of technology and how to protect the advantage of the technology transfer market, among other innovations. Norms will play an important role here too. NATO member nations need a

reevaluation of ethical and transparency principles, to also ensure that other civilian stakeholder, such as universities and private sector partners can work on security and defence emerging technologies.

An open question, addressed by Break-Out Group #2 and the Opening Panel, was whether the offense or the defence has the advantage in cyber operations.

Closing Remarks and Young Leaders

In closing, Floyd emphasized the importance of bringing together liberal arts with war studies, with computational breakthroughs like Artificial Intelligence and neural networks, and with the art of diplomacy, so nations may solidly navigate today's challenging and multifaceted geopolitical challenges that span physical, social, and cyberspace. The tenor of the event then shifted to the young leaders present today and their afternoon charge.

Vital to any conversation on tomorrow and cyber resilience is the next generation. Today's youth have been raised in this new world filled with ever evolving technology, security, and new challenges. This conference had three youth components.

First, young leaders ages 18 to 35 were fully involved participants in all portions.

Second, Closing Ceremonies included a report-out by undergraduate students Terra Stearns and Kiran Rachamallu from the 21 October 2022 virtual W&M Global Innovation Challenge (WMGIC) x NATO Headquarters Countering Disinformation Competition. During the competition, more than 400 students across NATO Member and Partner Nations pitched solutions to one of seven topics: Russia-Ukraine War, Public Health, Climate Change: Clean Energy, Climate Change: Climate Security, Artificial Intelligence, Gender-Based Violence, or Terrorism. Through the WMGIC x NATO HQ competition, participants and their solutions have been and will continue to be heard by practitioners and professionals around the world, including NATO leadership, with the promise of inspiring concrete action. Considering today's undergraduates' intense familiarity and upbringing in the digital world, there is no group better equipped to lead us in securing our information streams. The mind's of the competition participants combined with WMGIC's method extends a strong interdisciplinary approach to cyber resilience, cyber defence, and new technologies. This strength was seen in the WMGIC x NATO HQ competition, and will continue to be evident in the coming years as today's youth become tomorrow's leaders.

Design Thinking and Entrepreneurial Approaches to Cyber Defence Workshop
Third, the afternoon was devoted to a special "Design Thinking and Entrepreneurial Approaches to Cyber Defence" workshop reserved exclusively for youth engagement and lead by:

- Dr Amy Ertan, Cyber and Hybrid Policy Section (CHP), Emerging Security Challenges Division (ESC), NATO [Facilitator]
- Mr Graham Henshaw, Executive Director, Miller Entrepreneurship Center, William & Mary [Facilitator]
- Dr Anthony Stefanidis, Professor of Computer Science, William & Mary [Facilitator]

Participants were given a specific problem faced by NATO in the cyber defence realm. They were guided through how to apply design thinking to this task, then were given space to ideate as they worked through "How Might We" (HMW) questions on one of three problems.

Problem #1 addressed: a range of adversarial state/state-sponsored, criminal, and other malicious actors conduct cyber and hybrid attacks against targets to achieve strategic objectives. These attacks may range from traditional cybersecurity breaches to sophisticated disinformation campaigns. Traditional deterrence mechanisms don't work in the same way as with kinetic weapons (i.e. nuclear). As an Alliance of 30 nations, it is essential that NATO work together effectively to achieve its tactical, operational, and strategic objectives.

Problem #2 addressed: there is a significant shortage of skilled cyber-versed security experts in the workforce. Especially ones who can operate effectively in the overlap space of cyber technology and policy making. Nations report challenges relating to the recruitment and retention of skilled cyber experts, and significant attention is being dedicated to training future talent (including through schools and university programmes).

Problem #3 addressed: NATO and its Allies face an incredibly fast-moving threat landscape. One aspect of this relates to technological developments – where adversaries are making the most of changing cyber techniques and emerging disruptive technologies. NATO and its Allies face the challenge of predicting future security threats AND preparing adequately for them.

At the end of the workshop, participants pitched their solutions to the challenge as part of a group.

Darius Kölsch, Desk Officer for Science & Innovation, Institute for a Greater Europe: Our group discussed the general problem of emerging and disruptive technologies, and the corresponding challenge of NATO having to predict future technological developments. Specifically, we discussed the question "How might we enhance Allies' preparedness for future security threats?" Several different approaches were taken into consideration, including incentivizing academic immigration, expanding (/maintaining) high-tech export controls, and creating an overview of all emerging technologies. Ultimately, however, we settled on expanding red teaming. In particular, we suggest expanding the role of red teams outside of the military, and within critical infrastructure. Given that a substantial portion of critical infrastructure in NATO member states lies in the hands of private companies, it is crucial to expand the definition of red teaming to include the corporate realm. Red teaming, the concept that one simulates an attack on security systems in order to discover flaws, is not new; our proposal is to expand the scope of red teaming. Possible implementation could include NATO-certification or other support (e.g., funds, coordinating secretariats, dedicated public-private partnerships) for private red team companies, or the creation of a NATO Red Team beyond the cyber domain. PR campaigns supporting a culture of red teaming in society may be considered as well. It is acknowledged that the proposal likely is not the cheapest. We nonetheless chose it because the priorities we see for NATO, particularly in the light of crises such as the Ukraine war, are *proven* effectiveness and resilience, and that, ultimately, is best achieved through repeated application and testing.

Alexandros Goniadis, Cybersecurity Operations Officer, CERT-EU: Our team decided to ideate on the basis of Problem #2 and "how might we: pursue agile organizational solutions that optimize collaborative decision-making across technology and policy teams, in particular. The ideas focused on how to bridge the gap between technology and policy teams within an organisation in general and then within an organisation like the Red Cross in particular, taking into account the target/nature of the organisation, international focus and budget/resource limitations. The team used two criteria to categorise its ideas, which were the cost of implementation and organisational resistance, while we made the strategic choice of limiting the pool of shortlisted ideas on the basis of their low cost and low organisation resistance. We landed on two ideas that complement each other. A) Create a cell within the organisation where the technical and the policy level would meet regularly and collectively work on creating links between "the field" and policy, B) organically bring the Policy Team closer to the Technology team, rather than management/hierarchy in order to build trust, the feeling that both teams work for the same goal, so that the policy team would not be perceived as a remote entity/gatekeeper of information between the technical team and management.

Isabella Castro, Fulbright Scholar, Fulbright Commission in Belgium: Our group addressed the issue of enhancing cyber defence collaboration between states, academia and the private sector to promote interoperability with NATO members & partners in combating cyber and hybrid attacks. Our group sought out to find a solution that was both practical and strategic in facilitating collaboration while respecting sovereignty and private property. As a result, we arrived at a recommendation of creating an independent organization consisting of members from academic spheres, the private sector, and state actors. This organization would require members to discuss and create policy recommendations as well as new software/technological developments used to multilaterally deter cyber warfare. Members would act as individual representatives rather than representatives of their employers, thus allowing for diversity of thought but autonomy in decision making.

Participating students will receive an acknowledgement of participation from William & Mary.

Inquiries and requests for additional information can be directed to wgc@wm.edu.