CYBERSEC

EUROPEAN
CYBERSECURITY FORUM

Brussels 27.02.2018

# DEALING WITH CYBER DISRUPTION

BRUSSELS LEADERS' FORESIGHT

# SUMMARY

## European Cybersecurity Forum – CYBERSEC

CYBERSEC is a public policy conference dedicated to various aspects of cyberspace and cybersecurity in Europe. CYBERSEC is recognised as one of Europe's top 5 cybersecurity conferences. The 3rd edition of the Forum in October 2017 brought together record-breaking 150 speakers and more than 1,000 delegates from all over the world. Among them were policy-makers, top industry experts, global private sector leaders, investors, and technology startups.

## Dealing with cyber disruption – Brussels Leaders' Foresight

Following the CYBERSEC formula, the conference in Brussels was divided into four thematic streams: State, Defence, Business, and Future. Each stream compoased of a dedicated panel discussion and an on-stage interview or presentations focused on the most up-to-date cybersecurity challenges in order to present actionable recommendations and foresight of C-level actors in all aforementioned areas. Each panel followed a multi-stakeholder approach, bringing together the perspectives of both public and private sectors, as well as academia and independent experts.

The most urgent issues of cybersecurity policy, such as disinformation, EU-NATO cooperation and cyberdefence capacity building, cybersecurity certification or the role of AI in the cyber domain were debated by almost 40 the decision-makers of the EU and NATO, national governments and industry leaders at a conference attended by ca. 200 participants.

## Europe's cybersecurity – a decisive year

2018 is a crucial year for Europe's cybersecurity policy framework. It brings the implementation deadlines of both the General Data Protection Regulation (GDPR) and the Network and Information Security (NIS) Directive. Moreover, this will be a decisive year for the negotiations concerning the shape of the European Parliament's report on cyberdefence, the Commission's Communication on countering fake news and disinformation and finally – the Cybersecurity Act that not only enhances the EU's institutional capabilities, but also provides opportunity to stimulate the development of the secure-by-design Digital Single Market. Besides, 2018 will bring an unprecedented EU R&D investment within the European Defence Fund, which goes in line with the enhanced strategic cooperation between NATO and the EU, as entailed by the Common set of new proposals on the implementation of the EU-NATO Joint Declaration. Cyberdefence cooperation will be among the main topics of the NATO Summit in July 2018. Finally, the Commission will also put forward the necessary initiatives for strengthening the framework conditions to enable the EU to explore new markets through risk-based radical innovations, such as the Artificial Intelligence. CYBERSEC provided a platform to debate the development of Europe's cyber readiness at the beginning of this decisive year.

## Zooming in on the Central and Eastern Europe point of view

Improving connectivity, enhancing the competitiveness of the digital single market, developing smart economy based on free flow of data, strengthening cybersecurity and trust in digital services and privacy – the priorities set by the Bulgarian Presidency of the Council of the EU address the main civilisation challenges ahead of Europe.

As pointed out by Mariya Gabriel, European Commissioner for Digital Economy and Society: "future belongs to secure and connected Europe". This message is coherent with the agenda of the Central and Eastern European states who, on the one hand, perceive digitisation as the opportunity to boost the innovation and competitiveness of their economies, and on the other hand, need to enhance their cybersecurity capabilities due to dynamic evolution of the cyberthreat landscape as well as Russian disinformation and propaganda warfare. Given the regional push for digitisation and cybersecurity, as has already by proven by the Estonian presidency, the efforts of Central and Eastern European states are important contributions to the development of the digital agenda of the EU.

# STATE STREAM SUMMARY

## DISCUSSION PANEL: *No fake news is good news – disrupting truth in the digital age*

*A large part of dealing with the disinformation problem is the private sector's domain. We can address it if we strike an appropriate public-private cooperation in the field.*

**Julian King**, European Commissioner for Security Union

*Transatlantic cooperation is crucial, vital for the most important issues. For decades the main goal of the Kremlin was to dismantle the transatlantic alliance. The EU should not build additional institutions but enhance cooperation with NATO.*

**Anna Fotyga**, Member of the European Parliament

*We have to combat fake news with precision and caution in order to maintain a resilient, open society.*

**Marietje Schaake**, Member of the European Parliament

*Fake news factories and troll farms are not creating narratives. They exploit problems that already exist in Western society.*

**Andrei Soldatov**, Investigative Journalist
Russian Security Services Expert; Author of *The Red Web*

### DISCUSSION PANEL TAKEAWAYS:

- More EU-NATO cooperation is a key to combat state-orchestrated disinformation and fake news campaigns. Instead of building new agencies, interinstitutional cooperation should be enhanced. The European Centre of Excellence for Countering Hybrid Threats should serve as an example to follow. The EU should engage in a strategic cooperation with the NATO StratCom COE in Riga and NATO Cooperative Cyber Defence COE in Tallinn.
- Given the fact that digital platforms provide dissemination tools for spreading disinformation, the problem might be addressed effectively only if an appropriate public-private cooperation is established.
- Future-proof legislation is one of the key elements of the disinformation prevention toolbox. What is applicable in the offline realm should apply online too. This concerns legislation on hate speech, elections, advertising, consumer and data protection, as well as transparency of funding of political campaigns and political parties.
- Effective cooperation between public administrations and digital platforms could enhance the transparency of the latter. Due to the black box nature of digital platforms, there is an increasing information asymmetry between users (societies to an almost universal extent) and operators. Digital platforms are capable of leveraging their position against States' attempts to impose forms of public oversight, which poses a significant risk to democratic functioning and processes. On the other side, the scope and scale of possible misuse of digital platforms to disseminate targeted disinformation that might

effectively affect social behaviours (e.g. election results) call for immediate action that would prevent inter alia privatisation of law enforcement referring to the exercise the freedom of speech.

- The definition of fake news, disinformation or junk news needs to be precise and cautious. Although the phenomenon isn't new, the digital age brought unprecedented opportunity to disseminate targeted communication which affects human behaviour. In addressing the challenge, a great care has to be embedded in order to prevent possible infringements of the freedom of speech.
- Education aimed at increasing media literacy, critical thinking and digital skills is crucial to strengthening the social resilience towards disinformation. This is especially important in the context of the younger generation that consumes the majority of news via social media. They should gain the knowledge of how to recognise a credible source, verify the provided information, and maintain resilience in the rapidly changing media landscape that suffers from a growing information bubble. As long as media audiences are isolated, they aren't able to communicate and verify the information feeds that are delivered. On the other hand, information bubbles facilitate the creation of tailor-made targeted communication. Each filter bubble could be simply served with adequate content in order to achieve a given goal within the information warfare.

# DEFENCE STREAM SUMMARY

## ON-STAGE INTERVIEW: *NATO cyber readiness*

*Public attribution is important in terms of undermining the culture of impunity. Because we can't attribute, we can't take any punitive measures. But the whole question is how we go from a paradigm of cyberattacks which could bring a potentially enormous gain for extremely low risk in terms of attribution or penalty to another paradigm, where there would be a potentially very high risk of attribution, sanctions, actions, naming and shaming to less and less gain. Our resilience would have made these attacks less productive for the attacker.*

*All the conflicts in the future are going to have a cyber dimension. During the conflict, we are going to have a cyber bombardment day and night for a long period of time. We should be able to effectively negate, lock that degree of cyber bombardment to make sure that none of the important command-and-control networks or communication networks are disrupted.*

**Jamie Shea,** Deputy Assistant Secretary General for Emerging Security Challenges, NATO

### INTERVIEW TAKEAWAYS:

- Cyberthreats used to be considered an inconvenience that could easily be handled. Now, they are a potential existential danger – a strategic threat – to the confidentiality of intelligence sharing, to command-and-control, to weapons functionality, to systems, and to trust in data, particularly in sensitive military operations. Eventually, cyberattacks evolved from a side effect of military operations into a core element of them. Potential conflicts will necessarily have a cyber dimension. NATO will need to prepare for this.
- The attacks show the massive interconnectivity of the system, as they can spread rapidly. Consequently, interconnectivity implies a boomerang effect and might be a deterrent: the state could launch an

aggressive cyber campaign and become a victim itself. On the other hand, interconnectivity also stimulates cyberattacks as a kind of new vandalism which consists of hitting the target regardless of the consequences. It stands in opposition to the traditional warfare where one discriminates against particular targets and doesn't inflict collective damage against innocents.

- In cyber, public sector and law enforcement depend very much on outside sources of information and intelligence. Private sector often spots things earlier than national or international entities do because of their role with regards to civilian networks. In this context, NATO Industry Cyber Partnership was established with the aim to support the protection of NATO's networks and make NATO's in-house resources better and faster. Also, the European Union can possess information earlier than NATO, or inversely, according to the nature of the attack. Therefore, cooperation between these two is crucial. As an example, during the WannaCry attack, the input given by the industry and CERT-EU greatly supported the actions of the allies.
- Obtaining knowledge about network vulnerabilities and the origins of attacks takes a large degree of good state intelligence work. Not all allied countries are in a place to do it successfully, and NATO itself doesn't own all intelligence producing facilities. Cyber has been considered a confidential topic. Countries with the capabilities have been discreet about them and have not been willing to give a lot of information. NATO also signed 23 memoranda of understanding with individual allies which facilitate the exchange of information and provide means to create a mechanism for assistance in case of cyberattacks. Moreover, the Cyber Defence Pledge created a necessary climate of confidence among the allies so they can be open about their state of preparation. CDP also brings a serious benchmarking and maturity model system that allows countries to have a better sense of how they are doing vis-à-vis others. NATO now has a better idea about strong and weak sides in the individual countries, as well as the vulnerabilities that could impact on NATO operations. It is important because the military also depends on national critical infrastructure which could be targeted and impacted by a cyberattack during a military operation. Knowing weaknesses allows for the searching of solutions.
- The technology side is an issue because it moves incredibly quickly. Nowadays, we have to do technological upgrades more often than before. The problem is that a large number of extremely important public institutions are still operating with out-of-date software. They lack a strategy or they simply don't have resources to invest in new software. The attacks are a warning that there is a need to look at the areas of basic cybersecurity.
- The operalisation of cyberdefence provided NATO with four elements: the resilience mapping, the persistent defence system, the selective offensive counteraction tools, and an effective stratcom that deters the adversary from challenging you. These four need to be integrated with the necessary political oversight that NATO is working on.

## DISCUSSION PANEL: *EU and NATO cyber affair – joint transatlantic effort in cyberdefence*

*The EU finally decided to build a European Defence Union. One of the internal parts of this union is cyber. We realized that this is a very fast-growing risk and an adequate defence system cannot exist without cyberdefence. It is also obvious that the security and defence field here in Europe should develop with the EU and NATO going hand-in-hand.*

*The goal of the EU report of cyberdefence is to raise awareness about cybersecurity and cyberthreats. The report sends a signal to governments that this is an issue. There is not a sufficient number of decision-makers who take cybersecurity seriously. The report highlights the differences between member states in cybersecurity level and the difficulties in gaining cohesion between various national entities.*

**Urmas Paet**, Member of the European Parliament

*Security is only a preventive part of resilience. Security comprises protection against known threats against which we know how to defend ourselves. Resilience is more about unknown threats. But to achieve resilience, we need to start with security, cyber hygiene and minimum requirements.*

**George Sharkov**, Adviser on Cyber Defence, Ministry of Defence of Bulgaria

*We need to make sure that we have a binary actionality. It may be tempting for a government or an agency to see our vulnerability in the operating system or in an application as something that may be a cyberweapon that can be used in intelligence gathering, but if we do know the vulnerability and we do not at least share it with an organization that can fix it, we create an exposure.*

*The cloud can help in mission assurance. It adds redundancy and resiliency, as well as additional ways to get to the data in crisis management during the mission.*

**Diana Kelley**, Cybersecurity Field CTO, Microsoft

*The idea that there is an unchallenged way to defend yourself in the cybersecurity perspective is something that we need to divorce ourselves from. It is not a matter of 'if'; it is a matter of 'when'. Cyberattacks, regardless of their vector – whether they are state sponsored, whether they come from some sort of activists – they are going to happen.*

**Thomas Goodman**, Director, International Cyber Business, Raytheon

*There is a dynamic in the EU-NATO relation in general, but in cyber, there is a particular dynamic. Exchanging military concepts between the two organisations enables their development and the harmonization of processes. Technical cooperation leads to political interaction.*

**Sorin Ducaru,** Former Assistant Secretary General for Emerging Security Challenges, NATO

*Tallinn Manual 2.0 pointed that there is no possibility to establish collective cyber measures, as it is a right of individual nation-states. However, Article 4 of the North Atlantic Treaty may serve as a vehicle in this regard.*

**Wiesław Goździewicz**, Legal Adviser, NATO Joint Force Training Centre in Bydgoszcz

## DISCUSSION PANEL TAKEAWAYS:

- Cyberattacks are inevitable – this is a basic foundation of the new mind set when thinking about cybersecurity. In this regard, the art of continuing to operate while being attacked is a key tenet of being effective. However, being ready and being able to have some level of resilience underpins the need of common understanding among all actors of what resilience is and how to work the way through to defending yourself. Joint EU-NATO actions (e.g. exercises including the political/ministerial level) could contribute to the process.
- The main goal of the EU cyberdefence report that is being created is to raise awareness among European societies and policymakers in member states and in EU institutions. The document provides a sort of public diplomacy to give a clear signal to decision-makers, with regard to defence budgets planning. Increased cyberdefence capabilities serve the purpose of deterrence against potential hostile actors.
- Large amounts of information going over the networks, including hacks being launched, are viewed by large vendors and providers. This information needs to be shared out with nations and intelligence services when something suspicious is going on. It should be done in an immediate and automated manner because attackers move very quickly. Nevertheless, information sharing should be held reciprocally. It is critical that vendors share information; governments, when they do discover a vulnerability, need to report it. In a long run, this approach is going to make the network strong and more cyber resilient. The EU and NATO should act hand-in-hand and engage with the private sector in order to develop and maintain situational awareness and resilience mapping.
- We are all related, digitally dependent and vulnerable to shared cyber risks. At the end of the day, we are as strong as our weakest element. It is a subject that the Bulgarian presidency is working on through creation of an extended list of essential services and critical infrastructure in cyber that goes beyond NIS Directive requirements at the national level. The Bulgarian presidency is trying to align the language and taxonomy indicated in various legislations with regard to the response to attacks, the resolution, and the risk assessment that implies new hybrid threats and the Article 5 regime.
- We are entering an era with the predominant role of technology in the economy, social life, and security matters. Therefore, we have to look for a new type of a deep public-private partnership between governments and key industries that are powering this technological change. EU and NATO member states need to be open for such cooperation.
- The EU and NATO could better complement each other. For example, NATO has a crisis response manual and the EU is developing a cyber diplomacy toolbox. The two organizations should therefore work to better coordinate crisis response. Some areas could be shared by the two institutions, but in other areas cooperation in a more coherent manner would be the best solution.
- The current social and economic dependence on data is even more important in the context of military missions. The cloud enables one to continue to operate without access to any level of information feed; therefore, it may be very useful in mission assurance, especially during crisis management situations. The big issue that has to be addressed in the first place is the problem of contested information, especially in light of rising IoBT (Internet of Battlefield Things) application. What is most disrupting for military operations is not the lack of information but the situation when the information you have is not trustworthy.

# BUSINESS STREAM SUMMARY

## PRESENTATION: *Cloud-First Policies as a cybersecurity solution*

*In the past, people would typically store their money under their mattress, as they would consider it the safest place to store their money. Today, you obviously store money in a bank, as it is the safest place. You can make the same analogy with data. In the past, it was much safer for you to keep it in-house within your company, but the game has really changed. The safest place where you can keep your data today is in cloud services.*

**Pierre Chastanet**, Acting Head, Cloud & Software Unit, European Commission

### PRESENTATION TAKEAWAYS:

- European businesses are currently not fully reaping the benefits of cloud technology. Only 21% of European enterprises are using cloud services. Security remains their prime concern for not using the cloud. The second most important aspect is lack of trust and legal uncertainty. At the same time, cloud solutions can reduce IT costs for businesses between 20 and 50%. They can provide greater flexibility for companies, enable scale-up, and deploy their products and services across multiple countries. They provide IT resources in a flexible manner and provide on-demand capacity to these businesses without having to worry about all the technical complexity of having to put the IT infrastructure on the ground.
- The NIS Directive recognised cloud services as one of the digital service providers. In January 2018 the European Commission adopted an implementing act that established the security requirements for cloud services providers. Industry stakeholders contributed to the development of those security requirements. They are based on international standards so the companies could adapt quickly. On the one hand, they assure compliance with the NIS Directive, and on the other hand they safeguard maintain global service provision for cloud services.

## PRESENTATION: *Introductory presentation on the EU Cybersecurity Certification Framework*

*The benefit of certification in the future is first and foremost a much higher availability of transparent information about cybersecurity features of what consumers buy. Also, there would also be a great practical incentive for operators of essential services in the field of energy, transport, finance, etc. They could demonstrate that they are actually serious about risk management and security measures by using certified products and services.*

**Jakub Boratyński,** Head, Cybersecurity & Digital Privacy Unit, European Commission

### PRESENTATION TAKEAWAYS:

- Certification is by no means a guarantee for 100% cybersecurity because there is no such thing as 100% security. Nevertheless, it provides some methodology of testing or verifying features of a given ICT product or service that enables credible evaluation that contributes to increasing its cybersecurity.
- By default, the Cybersecurity Certification Framework as proposed by the European Commission is voluntary in nature and does not provide a ground for mandatory certification. In other words, the

companies would seek certificates not as a condition to put products on the market, but rather as a potential competitive advantage that proves high cybersecurity requirements that their offering meets. Also, the certification proposal aims at building a competitive advantage for "Made in Europe" products across the world as well as attracting vendors from third countries which would seek to be granted a European Cybersecurity Certificate as a brand of high quality and trust.

- The prime focus of the European Cybersecurity Certification is control systems in the critical sectors (operators of essential services). Other priority areas are mid-level security in widely deployed digital products as well as in mass consumer products, especially IoT-driven solutions.

## DISCUSSION PANEL: *Secure by design, certified by EU – IoT as the engine of the digitised European industry*

*When we legislate in the European Parliament, it is important to bear in mind that as much as we try to make our system secure, to a very large extent it is up to individual citizens. We should not underestimate that more than 95% of the vulnerability of cyberspace comes from cybersecurity incidents caused by human error. So I think that it's a good idea to include to the enlarged mandate of ENISA responsibilities related to raising awareness.*

**Eva Maydell,** Member of the European Parliament

*I think that without security by design, we will never be able to come up with really secure systems. Security needs to be considered from the very beginning of system development and design, by starting the technical design of specific solutions that ensure security by default.*

**Volkmar Lotz,** Senior Manager and Chief Research Strategist, SAP

*It's very important to create human-centred IoT – a technology which respects the core values and fundamental principles we have in Europe. This is actually where the question of security and privacy comes to the picture. The key word, I believe, is trust. What we want to do is to increase the trust of consumers and end-users, as well as the industry, in these IoT solutions.*

**Nikolaos Isaris,** Deputy Head, Internet of Things Unit, European Commission

*Certification does not bring trust. With the first breach of quality you lose complete credibility and this turns around – it becomes a dissatisfier. It is extremely important to be realistic about the fact that there is no perfect labelling whatsoever. We need to foster the education and involvement of end-users to raise awareness about possible risks and vulnerabilities.*

**Kees van der Klauw,** Chairman, Alliance for Internet of Things Innovation (AIOTI)

*A European Certification Framework would have a number of important objectives: To put into place the minimum security requirements for IoT to ensure it is kept up-to-date, to ensure compliance with those requirements, and perhaps to have a certification label or trust-mark for companies that can demonstrate compliance with those requirements, which would then increase consumer confidence.*

**Robert McDougall,** Head of Enterprise Public Policy, Vodafone

*With regards to the certification framework, sectors with varying maturity levels have different interests. As ECSO, we created the Meta-scheme approach in which we try to have some basic common understandings across different sectors.*

**Luigi Rebuffi,** Secretary General, European Cyber Security Organisation

*We cannot control the IoT revolution. What we can do is to implement standards and certified products and services to provide for a uniform approach towards the threats that come with the IoT devices introduced into our critical infrastructure. Maybe our current standards need to be re-evaluated in order to protect our critical infrastructure from the additional threats introduced by IoT.*

**Agnieszka Konkel,** Independent Expert

*We have a very short timeline to complete the Cybersecurity Certification Framework before the European Parliament finishes. Obviously, there are challenges.. We have a debate about the voluntary nature of certification, etc. Overall though, I think this is really coming together, and there is a political drive present in these negotiations.*

**Catherine Stihler,** Member of the European Parliament

## DISCUSSION PANEL TAKEAWAYS:

- Given the fact that more than 75 billion connected devices are expected to generate annual economic benefits of $11 trillion globally by 2025, while the market value of the IoT in the EU is expected to exceed one trillion euros in 2020, the EU action plan for IoT development is based on three pillars. Firstly, it stresses the importance of establishing a single and unified market for IoT. Secondly, it aims at building a dynamic ecosystem that enables technology to flourish and SMEs and large companies to develop. The third pillar is to build a human-centred IoT that is based on respect for core European values and fundamental rights including maintaining security standards and privacy protection. This should contribute to increasing trust towards IoT-driven solutions of end-users or consumers as well as industry.
- The EU cybersecurity certification should be future-proof and developed in a manner that guarantees flexibility that enables the introduction of innovative solutions. A balance between technological progress and necessary cybersecurity assurance has to be struck.
- The IoT has a profound role in the digitisation of the European economy. Nonetheless, in the recent Vodafone's IoT Barometer, security breaches and data privacy remain the top two concerns that hamper the development of the IoT (18% and 15%, respectively). This highlights the importance of the EU cybersecurity certification particularly with regards to the IoT. One area where certification could contribute is by setting minimum requirements to all actors in the supply chain. This could enhance the resilience of the whole ecosystem. Granting a certification label of trust to entities that comply with the requirements might significantly contribute to increased consumer confidence.
- Given the complexity and significance of the EU Cybersecurity Certification Framework and the Cybersecurity Act in general, as well as the approaching end of the current mandate of ENISA, it's crucial to finish the legislative process before the completion of the European Parliament's term in mid-2019. In the best-case scenario, the legislation should be passed this year in order to be harmonised with the currently negotiated EU Multiannual Financial Framework. This would demand a lot of discipline and effort on the part of lawmakers and stakeholders involved in consultations.
- Certification does not equal security. Firstly, it needs to be assured that certification schemes would include update procedures. Secondly, certification should be complemented with the involvement of end-users and transparency with regards to possible vulnerabilities, information sharing, as well as

education and raising awareness. In order to safeguard the credibility of cybersecurity certification, it should be resilient to possible (if not certain) breaches affecting certified devices.

- Certification schemes could also include best practices with regards to how certain processes are conducted. Even a system consisting of secure (certified) components is not secure *per se* as a whole. Therefore, cybersecurity certification might include best practices, methodologies, guidelines and codes of conduct that should be followed in order to safeguard cybersecurity of the developed ICT product or service. Such an approach could also guarantee flexibility and enable innovation (as long as it would focus on certain development procedures, not their result).
- It should be considered at a later stage during the process of drafting the European Commission implementing acts enacting certain certification schemes whether some of them shouldn't envisage mandatory approach in certain sectors (e.g. operators of essential services under the NIS Directive). A more interventionist approach based on the requirements of the critical infrastructure as well as its security risk assessment could complement the European cybersecurity system by increasing the level of actual implementation of the NIS Directive.
- The EU has to actively engage in standardisation efforts with third countries in order to make sure that they are developed internationally. As a result, the certification schemes will have the widest possible basis. Biannual EU dialogues dedicated to ICT with major trade partners could serve as a forum for such cooperation. Also, they might contribute to encouraging trade partners to follow EU's best practices in cybersecurity, data protection and privacy policies. Finally, industry should be invited to join the discussion in order to present the market perspective and safeguard the transparency of the process.
- Public administration could contribute to the actual implementation of cybersecurity certification through public procurement. It could set the example by inserting certain requirements in the procurement conditions. This would encourage contractors to obtain certification schemes in order to achieve competitive advantage.

# FUTURE STREAM SUMMARY

## ON-STAGE INTERVIEW: *Security through innovation – risk management in the era of AI and Big Data*

*When we look at technologies we currently have available, they can definitely help us in three major ways: predict when an attack can happen, where it can happen and prepare some response to the potential attack.*

*Interestingly enough, in 2016 and 2017 we started observing attacks that were fully automated and operated by machines on both sides. Hackers were using AI technologies to attack corporations, and corporations were also automated and used algorithms in the prevention.*

**Roman Pałac,** President of the Management Board, PZU Życie SA

### INTERVIEW TAKEAWAYS:

- Corporations are confronted with the question of what is more beneficial for them: to outsource the research and development activity or to do it internally. The outsourcing model is faster and sometimes cheaper, because an organisation pays only for the effects, not for the effort. Internal innovation is extremely difficult for large corporations. It requires careful recruiting and changes in people's attitudes; it is not an easy process. Therefore, both solutions are needed. Big companies cannot close doors and try to do everything internally. Nevertheless, there are some critical capabilities and processes that cannot be outsourced.

- There is a need to create proper communication with small and medium enterprises and start-ups. They have brilliant ideas but sometimes do not fully understand the business model of large corporations. For instance, in many cases technologies that are developed by start-ups outside of the financial sector can be easily applied in the financial sector, but those companies just do not realize that there is a business opportunity.
- While the cyber insurance market in Europe is just beginning to develop, an increasing need for this type of services may already be observed. Even non-digital industries are interested in solutions that would offer them frameworks to defend against cyberthreats. This is mainly due to still growing connectivity. There are more and more machines that are fully automated and controlled from remote locations.

## DISCUSSION PANEL: *The mission to keep robots accountable and safe – principles of AI development*

*I think there is also this idea that regulation will stifle the innovation, that regulators are "the bad guys" and they prevent everything from being pro-active. But on the other hand, if we want the AI-driven industry to fly, we need trust in the products, in the industry.*

**Mady Delvaux**, Member of the European Parliament

*If you develop AI, do it in a multi-stakeholder type of setting, think about that your AI may be used for good purposes and for bad purposes, think that it can have both civil use and military use.*

**Paul Timmers**, Visiting fellow, Oxford University

*Artificial intelligence is already impacting the cyberthreat landscape in the way we develop offensive and in the defensive tools used for cybersecurity. All of a sudden you are in a world where you have AI fighting AI, another AI defending that AI, and we live in science fiction.*

**Paweł Lawecki**, Boston Consulting Group

*Every year there is more data being produced than in all preceding years cumulatively.*

**Szymon Janota,** Business Unit Managing Director, Future Processing

## DISCUSSION PANEL TAKEAWAYS:

- A well-functioning society needs rules. The controversial issue is whether the regulation will stifle innovation. Regulators are sometimes perceived as "bad guys", but when something goes wrong, they are accused for not being conscious enough. A right balance needs to be struck on this issue. The assumption that 'law is bad for innovation' is not generally true. A common approach of the European

Union is necessary. The creation of fragmented national laws in Member States may create new barriers to the completion of the Digital Single Market and to consumer protection.

- Artificial intelligence is already impacting the cyberthreat landscape in both the development of offensive and defensive tools for cybersecurity. There are three major components of the defence side: (1) automatic detection (algorithms automatically detect previously unknown vulnerabilities), (2) active response (algorithms can trigger an intelligent response, they can try to limit the attack and cut off the connection; they can also do quite opposite and hold the person as long as possible to determine who that person is), (3) prevention (algorithms try to verify what are the vulnerabilities).
- Artificial intelligence is becoming an important asset within organisations' capabilities and as such is becoming a new vulnerability class. The question arises as to whether it is easier to defend or to attack. There are two narratives: (1) more pessimistic saying that the attacker has to be right just once and defenders have to be right all the time; (2) more optimistic: the amount of resources, people, assets working on the defence side is actually bigger.
- It is difficult to indicate where AI will be heading. As machine learning and deep learning are based upon large amounts of data, we need to look at sectors where this data is produced. At the same time, it must be the data that can be easily put together. There are sectors, such as the health sector, that have great potential to apply AI. They generate large amounts of data but unfortunately in a very fragmented way. Other sectors that generate a lot of data are definitely those where there is a lot money going around such as the financial sector (this is also where we see AI for security being applied), telecommunications, and electronic commerce.
- The other positive example of using AI is to employ it as an advisory system. Algorithms notify possible threats, and then security expert decides if this is the threat or not. The same applies to medical solutions in which systems can advise doctors, deciding neither on the diagnosis nor the treatment, but only to suggest what the problem is.

# WORKING LUNCH ON CYBERDEFENCE – KEY RECOMMENDATIONS

## 1) BUILDING TRUST

We are entering the intelligence era. From a strategic point of view, aggregating and sharing information, including classified information, enables the understanding of existing threats. A critical issue in this respect is trust, which constitutes a foundation for potential cooperation. Not only does trust allow the development of common policy responses within the EU and NATO, but it also allows national intelligence to be provided to NATO, as long as the Alliance itself has no relevant capabilities available and needs to rely on its members to acquire that intelligence.

Nonetheless, due to many legal limitations and the confidentiality of military missions, which are present even within multi- and bilateral agreements, sharing information remains a problem. What is more, when the information consists of anything more than the target, the trajectory, or the origins of the incident, it is most likely classified, which  implies further limitations. There is a need to achieve interoperability that would help to handle these limitations. NATO already possesses the tools to share information, such as the Cyber Information and Incident System (CIICS), but the platform is insufficient and limited to malware characteristics. Therefore, another special platform based on the common memoranda of understanding could be designed for like-minded nations to foster communication. Membership could be granted based on compliance with accountable rules defining a certain level of reliability and commitment to the responsibility to disclose information.

Interoperability of information is crucial. In order to achieve it, we need not only a technical platform but, above all, standards of the accuracy, importance and utility of information. Another factor is the right design of the information sharing process. This includes defining different levels of classification and sensitivity and using modern technologies, such as privacy-preserving computation and regulations defining the scope of information accessible for certain groups of actors.

However, any new platform or a new classification system is not going to solve all the problems that the international community is facing in developing cooperation in the field of cybersecurity information sharing. No platform is going to build trust. In the cybersecurity domain, the rules are the same as elsewhere: if you disclose what you should not disclose, or you do not disclose what you should disclose, the next time you will not gain the information you need. As a result, you will not able to function as a credible partner in the intelligence realm.

## 2) COMMUNITY OF INTEREST & COMMON PERCEPTION OF THREAT LANDSCAPE

The borderline between military and civilian sectors is blurring nowadays; so is the borderline between peace and war. Private and public sectors, civilians and military are all subjects of the same threats in cyberspace. Therefore, there is a need for a common operative framework, and a common situational awareness. This is hampered by the lack of a common interest or a commitment to defend common values. In order to create such a common operational interest, the Federated Mission Networking in NATO should be extended to cyber operations.

Nevertheless, what NATO can see happening in its own systems is limited. While the NCIRC has a good situational awareness, it is insignificant in comparison to industry. Consequently, NATO needs to further engage with private partners to enhance the Alliance’s capabilities and threat intelligence. Moreover, governments should be encouraged to share information between themselves more effectively in order to contribute to NATO’s overall situational awareness.

Another important challenge in this domain is to bring intelligence and ICT communities together to enhance common understanding. As long as CSIRTs bring the technical specific information about cyberthreats, it needs to be translated into proactive intelligence and recommendations. This could also contribute to the ability of military intelligence services to complement the situational awareness with an understanding of the adversaries' intent. As a result, governments can combine technical and intelligence analyses, compare data coming from different services and establish the full threat landscape.

## 3) RESPONSIBILITY TO SHARE AND COOPERATE

Information sharing should not be an end in itself, and data should not be the only thing to exchange. Cybersecurity becomes a team sport, in which all actors cooperate with one another through polling and sharing, including capabilities, such as attribution, and the elimination of barriers for interstate intelligence cooperation. This type of collaboration does not require extra institutional constructs, as the existing bi- and multilateral platforms and processes are sufficient, but should simply be used more effectively.

## 4) CATEGORISED DATA

It is very important to be able to model and categorise information in an automated manner. Data should be tagged and structured according to content (e.g. the IP addresses of bad actors). This could significantly contribute to the creation of sensitive target lists. Currently, data is usually stocked but not categorised, and put on unprotected channels, which generates further vulnerabilities. Therefore, bringing information in, tagging it and being able to search it emerges as a critical challenge.

It should be a subject of further regulation what information is essential, what kind of data the particular members of the system are able to input, and how to define the highest level of restriction that should apply to the collected information. Additionally, an operational model of deleting data that does not need to be collected or used against this backdrop should be developed. It  is worth highlighting that data needs to be specific in order to be useful for the intelligence community.

## 5) DEVELOPMENT OF ATTRIBUTION CAPABILITIES AND RESPONSE OPTIONS

Given the difficulty to distinguish between war and peace in cyberspace, using attribution as a prerequisite for state responsibility for international acts is even more important below the threshold of the armed attack under Article 5 of the NATO Treaty. Nevertheless, NATO has not yet tested how to collectively adopt countermeasures in such situations, even though they imply a great risk of a quick escalation

The essential condition to develop a solid basis for NATO decision-making in different scenarios is to improve the Alliance's attribution capabilities. This will enhance NATO's ability to collectively respond to cyber aggression and develop diverse response options, which do not necessarily involve symmetric countermeasures. Including the cyber domain in a multi-deterrence strategy could effectively strengthen response capabilities. What slows down the process at the moment is limiting deterrence to the communication strategy that discloses our response capabilities.

In this context, it is crucial to develop partnerships with associated countries, such as Georgia, Ukraine and the Republic of Moldova as long as they could contribute to an extending resilience of the NATO security environment and bring unique expertise as well as lessons learned. Joint capacity building projects could serve as perfect platforms for the exchange of best practices.

In partnership with:

# SAVE THE DATE 8–9 OCTOBER 2018

#CSEU18 www.cybersecforum.eu