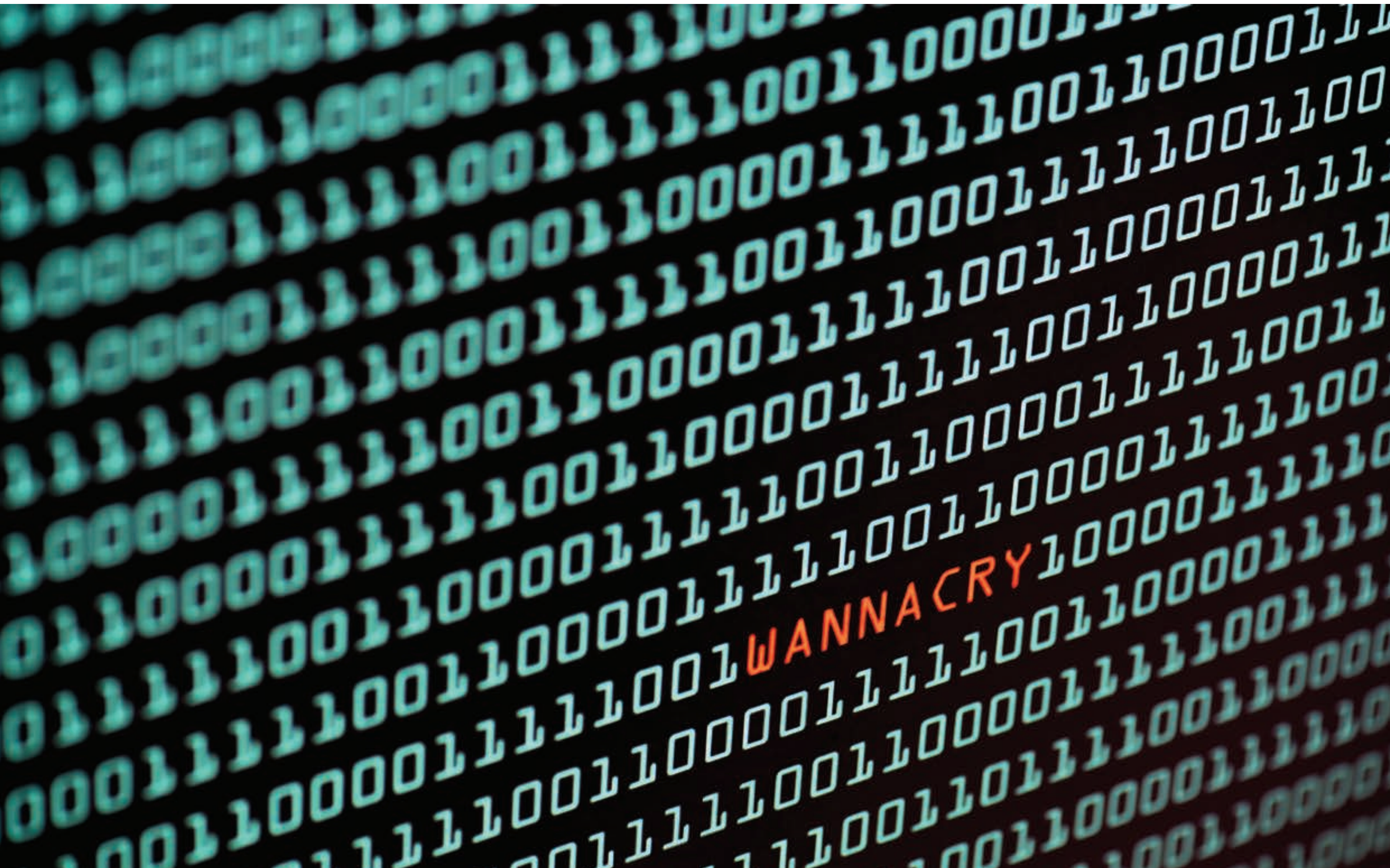
friends of europe

WINTER 2018

BUILDING CYBER RESILIENCE

ALIGNING STRATEGIES AND INCREASING COOPERATION

REPORT



This event is part of Friends of Europe's Peace, Security and Defence Programme supported by the United States European Command (EUCOM). Our work is firmly anchored in our expertise in a range of fields, including energy and climate change, geopolitics, international development, migration and health. We seek a holistic approach to European, transatlantic and global security policies. Security considerations are, in turn, mainstreamed into these areas of expertise, enriching the debate by encouraging experts to think outside their comfort zones.

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Co-funded by the
Europe for Citizens Programme
of the European Union

INTRODUCTION

Europe's latest cyber defence plans and projects are reason for cautious optimism, according to a panel of cyber experts gathered in Brussels on 6 November 2018 for 'Building cyber resilience: aligning strategies and increasing cooperation', the third Friends of Europe debate on resilience. "The empire seems to be striking back, thanks to the EU's playbook of responsive measures to improve resilience, deterrence and to hold cyber-attackers to account," said Jamie Shea, Senior Fellow at Friends of Europe.

Disruptive and malicious cyberattacks increasingly threaten our lives and society at every level. They cost the world €235 billion in 2017, with the NotPetya attack alone racking up corporate losses in the hundreds of millions. The WannaCry ransomware attack perpetrated by North Korea infected 300,000 computers across 150 countries and brought chaos to the United Kingdom's National Health Service hospitals. Deterrence and resilience are key to being able to withstand, recover and respond to these malicious assaults.

Building on the 2016 Warsaw Joint Declaration, the European Union and NATO have stepped up their cybersecurity measures and capabilities. These include extended partnership – such as coordinated exercises ranging from prevention, crisis management and recovery – and even the prospect of striking back at cyber foes. Yet, is the EU-NATO cooperation mature enough to enable both organisations to make a comprehensive contribution to cybersecurity? And are current international norms enough to govern conduct in cyberspace? There is also concern about Europe's ability to secure its cyber domain, given the new threats emerging alongside technologies like 5G and artificial intelligence (AI).

> **"The empire seems to be striking back, thanks to the EU's playbook of responsive measures to improve resilience, deterrence and to hold cyber-attackers to account"**
>
> **Jamie Shea**
> Senior Fellow at
> Friends of Europe

STEPPING UP EUROPE'S CYBER RESPONSE

In 2016, NATO signed a Technical Arrangement on cyber defence cooperation with the EU, while NATO Allies made a Cyber Defence Pledge to enhance their cyber defences. The EU boasts an ever-expanding playbook of cyber defence measures, such as the €13 billion European Defence Fund, EU Cyber Rapid Response Force teams and Permanent Structured Cooperation (PESCO) on security and defence. There is also new EU-wide legislation on cybersecurity, centred round the 2016 NIS Directive on the security of network and information systems.

Over the last year, the EU and NATO have also enhanced cooperation to ensure complementarity of measures, under the EU Joint Framework on countering hybrid threats. This framework aims to improve situational awareness, resilience of critical infrastructure (e.g. transport, communications, health services, energy, banking and finance) and responses from the EU and member states.

Cyberattacks on Estonia in 2007 were a huge wake-up call for Europe. Is the country better prepared for them today? "Cybersecurity is a cross-border issue. Estonia is more resilient today, thanks to better coordination and international policies on cybersecurity, especially at EU and NATO levels," replied Heli Tiirmaa-Klaar, Estonian Ambassador for Cyber Security. For example, the country's maritime sector escaped the tsunami-like damage of a cyberattack that recently hit a quarter of the world's shipping and ports industry.

> **"Cybersecurity is a cross-border issue. Estonia is more resilient today, thanks to better coordination and international policies on cybersecurity, especially at EU and NATO levels"**
>
> **Heli Tiirmaa-Klaar**
> Estonian Ambassador for Cyber Security

KEYBOARD CYBERWARRIORS

Estonia can also rely on the skills of its Defence League's Cyber Unit, whose volunteer specialists (including many IT professionals) protect national cyberspace, in cooperation with the government. The UK, France and the Netherlands too now have 'cybercitizen armies', complementary to military initiatives and cyber defence agencies springing up across Europe.

Where then does Europe stand on cybersecurity today? "The focus is on better preparation for cyberattacks through exchange of information, underpinned by the NIS Directive," said Vivian Loonela, Member of Cabinet of Andrus Ansip, Vice-President for the Digital Single Market at the European Commission. She also highlighted a push for better hardware and software, with a proposal for substantial cybersecurity investments in the next EU budget. "Cyber hygiene is also important, because we're all responsible for securing our computers and networks," remarked Loonela. She noted a growing public awareness of cyber risks, reflected in the fact that cyber features on the agenda of every European Council meeting.

> **"The focus is on better preparation for cyberattacks through exchange of information, underpinned by the NIS Directive"**
>
> **Vivian Loonela**
> Member of Cabinet of Andrus Ansip, Vice-President for the Digital Single Market at the European Commission

The EU is doing everything it can to boost cybersecurity, and that includes driving the Digital Agenda, said Loonela. "There are two million IT jobs going unfilled in Europe, due to the difficulty of finding people with appropriate skills," she noted. "We need more digital education and training, which will also empower our citizens to fend off cyber threats at every level." NATO is improving its cyber education and training and the skill sets of its operators, including through the setting up of a cyber academy at the CIS School, remarked Sorin Ducaru, Chairman of the NATO Secretary-General's Senior Advisory Board for the Functional Review of the NATO Headquarters, Special Advisor at the Global Commission on the Stability of Cyberspace, and Trustee of Friends of Europe.

Asked how NATO's Cyber Defence Pledge helps the Alliance's members, Ducaru picked out three advantages. Firstly, the pledge has got European leaders talking about cybersecurity and put it at the centre stage of politics. It has also set some related standards beyond military infrastructure. Lastly, it has led to cyber defence capability development and better institutional frameworks in NATO countries. Even better, a 2018 review indicated the pledge is stimulating inter-government and inter-agency work and cooperation on cyber defence.

"NATO has declared cyber as an operational domain, keeping the resilience focus while understanding that the Alliance must now take a broader approach," said Sorin Ducaru. Practically speaking, that means a "mission assurance paradigm", where it is accepted that a cyberattack will degrade some systems. However, thanks to systems redundancy and other capabilities, it should still be possible for NATO members to complete their mission goals. "So NATO may employ offensive capabilities, but always within international law through a defensive mandate, its major objective for the last seven decades," he added.

Ducaru said that NATO is now considering "imposing costs" for a cyberattack that hits a member country: "NATO links cyber defence to its core business, so could respond when cyberattacks reach the threshold of armed attacks or if they have the same implications as conventional attacks, in accordance with Article 5 on collective self-defence." On the EU side, several countries named and shamed Russia for its state-hacking activities: "It remains to be seen if this measure, or using attribution and economic sanctions, will assist our bloc's cyber defence," said Vivian Loonela, from the European Commission.

After noting his support of EU-NATO cooperation, with cyber at the forefront, Ducaru welcomed the EU's "cyber diplomacy toolbox" – a range of diplomatic, political and economic assets that could be wielded to retaliate against a cyberattack on the bloc. Among other technical and political measures, NATO and the EU are developing cybersecurity rapid response teams for mitigation, forensics, and sharing information.

"There are two million IT jobs going unfilled in Europe, due to the difficulty of finding people with appropriate skills. We need more digital education and training, which will also empower our citizens to fend off cyber threats at every level"

Vivian Loonela
Member of Cabinet of Andrus Ansip,
Vice-President for the Digital Single
Market at the European Commission

"NATO has declared cyber as an operational domain, keeping the resilience focus while understanding that the Alliance must now take a broader approach"

Sorin Ducaru
Chairman of the NATO Secretary-General's
Senior Advisory Board for the Functional Review
of the NATO Headquarters, Special Advisor
at the Global Commission on the Stability of
Cyberspace and Trustee of Friends of Europe

"We must also create a market for secure-by-design and educate consumers about the importance of secure devices and mobile apps, possibly through a new labelling system"

Ruth Davis
Head of Commercial Strategy and Public Policy at BT Security

BOLSTERING THE CONTRIBUTION OF BUSINESSES

The private sector is eager to play a larger role in cybersecurity. Ruth Davis, Head of Commercial Strategy and Public Policy at BT Security, said: "As a provider of the UK's critical national telecoms infrastructure, we focus on securing our networks because security is integral to our business." However, the company is also ready to share information on cyberattacks with its competitors and intelligence agencies. For instance, it can pin down ("attribute") the source of any cyberattacks by scanning BT's global networks.

"There is no uniform approach to cybersecurity across the private sector," added Davis. She noted how BT ensures all its products undergo a full security review before getting their "security passport". The UK government has also launched voluntary secure-by-design guidance for Internet of Things (IoT) manufacturers. But if product certification like this is to be effective, it may have to become mandatory. "We must also create a market for secure-by-design and educate consumers about the importance of secure devices and mobile apps, possibly through a new labelling system," said Davis.

There are both opportunities and challenges about the possible impact of next-generation 5G telecoms networks, AI and cloud computing: "These sophisticated technologies can be vectors for further cyberattacks, yet they also promise more resilient networking and cyber solutions such as stronger encryption."

CYBER DEFENCE: WHAT ELSE IS IN THE TOOLKIT?

While investing in cyber defence is a major economic cost for governments, this can be addressed through more public-private partnerships as well as further NATO and EU investments. Other solutions for cyber defence could include safer software, security throughout supply chains and active cyber defence by strengthening web infrastructure and protocols. There was consensus too on the value of the EU General Data Protection Regulation (GDPR), which has focused people's minds on security, privacy and data ownership in Europe and beyond.

"International law applies to cyberspace, though we don't yet know how exactly. The UN and many governments are slowly developing norms on cyber behaviour, which we can then build on," said Heli Tiirmaa-Klaar, Estonian Ambassador for Cyber Security. "We need to work on all aspects of cybersecurity, since there is no silver bullet on the horizon," concluded Jamie Shea. He underlined the inevitability of serious cyberattacks in the future. However, thanks to growing awareness of this risk, NATO and the EU are coming together more in the virtual space and further developing their counter-measure responses.

friends of europe
BUILDING CYBER RESILIE
ALIGNING STRATEGIES AND IN
SHARE THE PHOTOS

RECOMMENDATIONS

Invest in digital education and training: Building a strong EU cyber skills base is part of the European Commission's Cyber Strategy with the aim of empowering citizens to fend off cyber threats at every level. This requires developing cyber training of the workforce, additional cybersecurity training for tech specialists and introduce new specific cybersecurity curricula. The goal is to ensure that it becomes natural to design digitally connected products which incorporate and respect security standards from the very beginning. Better cyber hygiene needs to be adopted by individuals, businesses and organisations.

Create a market for "security-by-design" products: The private sector can play an important role in helping the European Commission in its implementation of an EU cybersecurity certification framework. A "security-by-design" approach could be used for connected devices to ensure that cybersecurity is addressed before any product is put on the market. Initiatives such as the EU NIS Directive, the GDPR and NATO's Cyber Defence Pledge have important roles to play here. This would benefit businesses as well, as they would avoid going through several certification processes. Ultimately, this new labelling system will incentivise the creation of more resilient networking and cyber solutions such as stronger encryption.

Apply international law in cyberspace: While cyberspace has often been referred to as a "jungle" or the "Wild Wild West", clear international cyber norms do exist and have been developed throughout the process of the UN Group of Governmental Experts (GGE). It is important that the normative framework for cyber behaviour is respected and needs to be implemented. In this context, the Tallinn Manuals serve as an important framework for Governments to follow. While legal definitions are crucial, attempts to establish a global convention of some sorts on cybersecurity are likely to get bogged down for years, so small scale or sectoral approaches are important parallel measures to take.

Protect critical infrastructure: Attacks on critical infrastructure, like the WannaCry and NotPetya attacks, demonstrate the devastating effect of malicious assaults. In order to improve their critical infrastructure resilience strategies, states need to refine and implement industry standards for cybersecurity in IT and banking systems, government services, the military, utility providers including energy and telecom companies, hospitals, transport enablers such as air traffic control and navigation systems, and so on. If resiliency measures are robust and publicly known, then it may have the effect of persuading malicious actors that their cyberattacks are unlikely to have the devastating effect they wish to inflict.

Image credits
Cover image: shutter2u/Bigstock
p8: Rawpixel.com/Bigstock

Friends of Europe
Connect. Debate. Change.

+32 2 300 29 92
info@friendsofeurope.org
friendsofeurope.org