WINTER 2018

HYBRID AND TRANSNATIONAL THREATS

DISCUSSION PAPER

friends of europe

This publication is part of Friends of Europe's Peace, Security & Defence programme. In this discussion paper, you will find perspectives and recommendations by a number of actors working on different areas of hybrid warfare and cybersecurity, featuring contributions from international organisations, national governments, academics and business representatives.

The Peace, Security & Defence programme is supported by the United States European Command.

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

WINTER 2018

HYBRID AND TRANSNATIONAL THREATS

DISCUSSION PAPER

friends of europe

Publisher: Geert Cami
Senior Fellow: Jamie Shea
Programme Manager: Mikaela d'Angelo
Programme Assistant: Gerard Huerta
Editor: Iiris André, Robert Arenella
Design: Elza Lőw

TABLE OF CONTENTS

FOREWORD

WE NEED TO BUILD RESILIENCE, DETERRENCE AND RESPONSES TO FACE THE INCREASING HYBRID THREATS

There are three types of hybrid warfare. The first, often labelled as an attack on governance, uses legal means to undermine democratic liberal societies by inserting foreign influence or trying to gain financial and economic leverage over our normal democratic processes. Examples of this type of influencing are all around us: Russian television stations or news agencies and China's 10% ownership of EU ports as well as its assertive presence in the South China Sea. To successfully respond, we have no other choice than making sure that we are working hard to assert our own democratic values and economic models. We simply need to out-communicate and outbid our adversaries.

The second type of hybrid warfare consists of the more brazen, illegal attempts to undermine and polarise our societies by sowing fear and mistrust. This is achieved by carrying out orchestrated attacks against the core elements of our social cohesion: free and fair elections, critical infrastructure and IT networks, the credibility of news and information, and the integrity of our business and financial transactions. Sometimes citizens become the direct target, as demonstrated by the poisoning of the Skripals in Salisbury.

The third – and the most dangerous – type of hybrid warfare means using the aforementioned strategies as preparation and prelude for a military attack. This happened in Ukraine in March 2014 when Russian Special Forces, posing as "little green men", seized the institutions, transport links, ports and communication channels of Crimea, thus preventing a Ukrainian response. While conflicts of

the past began with an artillery barrage or an air strike, future wars will almost inevitably start with a massive cyberattack or a swarm of drones and robots. Other examples of this method of combat include furtive stratagems such as Chinese spies infiltrating major US companies, North Korean cyber forces instigating ideological attacks and global players threatening the critical infrastructure of countries such as South Korea and the United States.

While these three types of hybrid activity should not be confused, it is our capacity to deter, limit and quickly recover from such attacks that will be of paramount importance. To this end, we must develop and build competences in the sectors of situational awareness and critical infrastructure. Governments and societies should also adapt and mitigate the threat by restoring trust in mainstream politics. While the EU and NATO are off to a good start, there is still a lot they can do – alone and together – and the EU-NATO playbook of measures to fight and manage hybrid attacks should still be expanded.

To address this timely and crucial issue, Friends of Europe is contributing to the global conversation on hybrid and transnational threats. In this discussion paper, you will find perspectives and recommendations by a number of actors working on different areas of hybrid warfare and cybersecurity, featuring contributions from international organisations, national governments, academics and business representatives.

Happy reading,

Jamie Shea
Senior Fellow at Friends of Europe

RECOMMENDATIONS

These recommendations to European and international policymakers draw on the viewpoints and ideas put forward by the authors in this discussion paper.

1. ENSURE BETTER EARLY WARNING AND FORESIGHT MECHANISMS

As disinformation and hybrid campaigns are often unpredictable and deliberately confusing, it is important to detect them as early as possible. Governments, but also the police, media, the private sector and civil society groups, need to improve detection and analytical capabilities, basing their findings on comprehensive monitoring and data gathering. This means investing in both the tools needed to detect the hostile narratives that are gaining momentum and in the experts needed to make sense of this information. This will undeniably require more resources and investment. Greater information-sharing between governments and the private sector, between military and civilian stakeholder communities, and between international bodies, such as the EU and NATO, will be crucial to achieving this objective. Additionally, a good bottom-up approach for information gathering and alert networks needs to be encouraged as hybrid activity is often first spotted at local level. A more integrated political response to detecting threats would allow for a faster and more effective response which would better mitigate the impact of a campaign, or attack, once it takes place.

2. IDENTIFY AND DEBUNK FALSE NARRATIVES

Fake news and disinformation campaigns undertaken by broadcasters, disinformation services and online trolls – whether from authoritarian regimes, extremist groups or populist politicians – have increasingly gained ground. The multiplicity of (dis)information is a clear security challenge which undermines faith in mainstream politics. The EU and its member states need to build on their strategic communications strategy, continue to catalogue and analyse the tools, techniques and intentions of the malicious campaigns and raise awareness of them. The European External Action Service (EEAS) has developed a strategic communication tool and response to hybrid threats through its "EUvsDisinfo" initiative which is also present on social media. Governments need to utilise proper risk assessments to determine the overall challenge external disinformation poses to Europe and incorporate the analysis of intelligence-based EU bodies, such as the Hybrid Fusion Cell. By being able to better identify and debunk false narratives, European leaders will be able to develop and promote a compelling and positive counter-narrative about what the EU's policies seek to achieve and how they provide benefits to its citizens. This will help Europe work on restoring trust and confidence.

3. DEVELOP AND DEFINE INDUSTRY STANDARDS TO 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 telecoms companies, hospitals, transport enablers such as air traffic control and navigation systems, and so on. 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, and to benefit businesses as well. Ultimately, this new labelling system will incentivise the creation of more resilient networking and cyber-solutions such as stronger encryption. By expecting a degree of inherent security, we can make Europe more secure against cyberattacks.

4. IDENTIFY OPERATIONS AND CAPABILITIES TO BE DEPLOYED IN THE CASE OF AN ATTACK

A key priority for governments should be to identify those national and international assets which can be sent to allies and partners in the event they experience a hybrid attack. As policies and approaches continue to evolve, both NATO and the EU are paying more attention to how they are equipped to manage and respond to potential crises. This is especially important as many cyber and hybrid activities are designed to fall below the NATO Article 5 threshold. The EU and NATO are, for instance, developing counter hybrid support teams to better prepare for an attack, as well as holding multinational exercises designed to improve their ability to manage hybrid crises and train the technical skills of those at operational level. These operations help build resilience into systems and can minimise the impact of an attack and enable the target to recover in a timely and efficient manner so that they can resume their operations. If resiliency measures are robust and publicly known, then it may have the effect of persuading a malicious actor that its cyber attack is unlikely to have the devastating effect they wish to inflict. These activities have a deterrent effect of dissuading potential hybrid or cyber practitioners from wasting their time and resources into planning a potentially ineffective attack in the first place.

5. EXPAND THE EU AND NATO'S ARSENAL OF POTENTIAL RESPONSES FOR HYBRID ATTACKS

While frameworks for responding to hybrid threats have been put in place at the international level, the EU and NATO are concurrently reviewing their respective diplomatic toolboxes in a bid to expand their response options. The EU is primarily stepping up its cooperation with NATO: the two organisations signed a technical agreement to strengthen their computer response capabilities and are conducting table top exercises to harmonise their procedures and working cultures. Both have also been coordinating on hybrid warfare scenarios and responses. Be it through information exchange, workshops or parallel and coordinated exercises like CYBRID (a strategic table top cyber defence exercise that was conducted in late 2017), the EU and NATO should continue working toward complementarity capabilities and avoid unnecessary duplication. Deepening cooperation between the two organisations makes a substantial contribution to preventing and responding to hybrid attacks. By doing so, the overall resilience against hybrid attacks is considerably increased.

6. RESTORE PUBLIC TRUST IN LIBERAL DEMOCRACY AND THE EU PROJECT

Hybrid warfare works by exploiting the polarisation of societies and the lack of public trust in their governments. More needs to be done at EU level to restore trust in centrist politics. To restore public trust in liberal democracy and the EU project, the EU and its member state governments need to get better at developing and promoting a compelling positive counter narrative of what their policies seek to achieve and the concrete benefits they can bring to the people. EU leaders need to sincerely communicate with citizens: they need to focus on tangible benefits the organisation provides instead of justifying its costs, and seek the help of trusted and authentic local multipliers to reach the audiences that governments have struggled to engage in the past. In this endeavour, the EU should not forget its commitment to the values of tolerance, democracy and human rights. This will ensure that citizens do not lose trust in the EU, in NATO and the membership of their countries within those organisations.

PART 1:
HYBRID THREATS IN ACTION: WHAT'S IN THE TOOLKIT?

It's all about governance: addressing hybrid and transnational threats

Private entities are often the first targets of a hybrid campaign

Christopher Kremidas-Courtney, the Multilateral Cooperative Engagement Coordinator at US European Command

Today, state and non-state actors are challenging nations, institutions and private companies through a wide range of overt and covert activities targeted at their vulnerabilities. Both NATO and the European Union refer to these as hybrid threats.

There are a wide range of measures in hybrid campaigns, ranging from cyber-attacks and disinformation to the disruption of critical services, such as energy supplies or financial services; the undermining of public trust in governmental institutions; and exploiting social vulnerabilities. Once a state is weakened sufficiently, the aggressor's strategic aims can be consummated by the use of conventional or paramilitary forces.

As we have seen recently in Crimea and the South China Sea, a hybrid approach lowers the political price for aggression, making regime change and territorial annexation possible 'on the cheap'.

Many refer to this phenomenon as 'hybrid warfare' and in the process 'militarise' the concept, which is actually much broader and more complex in nature. A whole-of-government and whole-of-society approach is needed to access the necessary means and authorities to address this phenomenon. Thus, hybrid threats are best understood as an attack on governance – specifically democratic governance.

Such threats have always existed, of course, but what makes them different are the new vulnerabilities presented by a globalised and more interconnected world; instant global communications; a globally connected system of finance and commerce; and interconnectivity of gas and electricity distribution grids across borders. Hybrid threats represent the weaponisation of globalisation.

In the South China Sea, Beijing seeks to establish its own governance over the territory. The rest of the international community endeavours to maintain the recognition of international waters, while Vietnam and the Philippines seek to maintain governance over their own territorial waters and exclusive economic zones (EEZ).

The governance which is challenged by hybrid threats is not just public but private as well. The majority of the world's supply chain, communication providers, financial systems and media outlets, operate in the private sector. They are the first targets of a hybrid campaign and even when they are not the main target, their vulnerabilities can quickly threaten global governance.

For example, a cyber-attack on the government of Ukraine in 2017 inadvertently impacted Danish global shipping giant Maersk. As a result, Maersk's global operations came to a halt as they temporarily lost the ability to govern their fleet and numerous other industries were also impacted as the global supply chain was disrupted.

In many western countries, 80-90% of all critical infrastructure is owned and operated by the private sector, and it is widely recognised that these private entities are often the first targets of a hybrid campaign. Given NATO's heavy reliance on the private sector to provide logistics and communications capabilities during a crisis, these vulnerabilities can have far-reaching political and economic effects.

Transnational threats are similar to hybrid threats in that they are also a threat to governance, Defined as threats such as organised crime, terrorism, illicit trafficking in humans, drugs, weapons and cybercrime, this broad group of challenges can also take the form of proliferation of weapons of mass destruction (WMD).

Transnational organised crime refers to self-sustaining groups that operate transnationally to obtain power, influence and commercial gains. This is usually completely or partly illegal in nature. They seek to weaken governance to enable them to act with impunity — moving materials, people, and money in and around governing regimes in order to conduct illicit commerce.

In building, maintaining and growing this system of impunity, transnational threats manage to corrupt government officials, computer systems, financial institutions, and deny governments the ability to control their sovereign borders and EEZ's. This in turn weakens their ability to collect taxes and customs fees to fund the execution of governmental functions and services.

Terrorists require the same system of impunity outside of governing frameworks to move people, weapons, and to coordinate their activities. Additionally, terrorists also require the ability to get their message out in order to recruit new members and gain the maximum attention for their actions.

Terrorists also present a challenge to governance as they stress the system to respond. This often results in harsh responses, disrupted economic activity and reduced freedom of movement for citizens. All these outcomes can drive a wedge between the people and their government.

Governments and public and private institutions with weak governance, are more susceptible to hybrid and transnational threats. They are subjected to corruption; low levels of public trust; weak public and private accountability; ineffective law enforcement; weak security protocols for critical infrastructure; and a lack of cooperation between ministries, institutions, and the private sector.

The answer to both hybrid and transnational threats is simple: building and maintaining resilient, credible and capable governance. This requires cooperation from all entities to achieve success. Strong public and private governance presents a credible deterrence to both hybrid and transnational threats.

In order for this to be achieved, many components are necessary. For example, these include participatory, representative and inclusive political processes and government institutions; accountability of leaders and institutions to citizens and the rule of law; competent, capable, and trusted law enforcement and justice systems; continuing efforts to build greater social cohesion and mutual trust; a free and accountable media sector; respect for universally recognised human rights; sound corporate governance, security, and accounting standards; strong inter-ministerial cooperation and information sharing; public-private partnership; cooperation; and information sharing to thwart, detect, attribute, respond, and recover from hybrid and transnational threats.

Beyond these, there are three levels of cooperation and collaboration that enable governments and societies to better deter hybrid and transnational threats:

First, a 'whole-of-government' approach, in which all agencies and ministries from national to local level cooperate and share information.

Second, a 'whole-of-society' approach, which is similar to the first, but also includes engagement with the private sector, academia and civil society.

And lastly, the 'comprehensive approach' that means like-minded groups or states working together with international organisations and entities such as NATO, the EU, OSCE, the UN, the World Bank, ICRC, the private sector and civil society. Each collaborate and coordinate to face challenges together.

By focusing on governance, instead of looking at hybrid and transnational threats through a military lens, one gains the perspective which more closely aligns with each nation's own legal authorities and frameworks and does not necessarily exclude a role for military capabilities. Given the nature of these threats, the first to detect and respond are most likely to be civilian government or private entities. In turn, this may require varying degrees of military capabilities to provide support. This cooperation is vital because no government wants to pay for the same capabilities twice.

In the event of a possibly escalating situation, close civil-military cooperation and interoperability is necessary to ensure an appropriate response, accompanied with all necessary and available instruments of national and international power and influence.

For this reason, comprehensive and whole-of-society approaches are vital to building trust and interoperability, while any gaps and vulnerabilities in our legal and procedural frameworks need to also be identified and closed. This can be best achieved through scenario-based discussions and table top exercises among various stakeholders.

Through strengthening public and private governance, and seeking deeper and broader cooperation among institutions, nations, and civil society, we can turn globalisation and our greater interconnectedness from vulnerability into an advantage.

The views presented in this paper represent the author's personal findings and do not represent the official views or policy of EUCOM or the United States government.

NATO-EU cooperation is essential to prevent hybrid attacks

Both NATO and the EU have made significant progress in recent years to address rapidly evolving security challenges

Antonio Missiroli, NATO Assistant Secretary General, Emerging Security Challenges
Irma Kaljulaid, Policy Advisor, Emerging Security Challenges

"We face a dangerous, unpredictable, and fluid security environment, with enduring challenges and threats from all strategic directions; from state and non-state actors; from military forces; and from terrorist, cyber, and hybrid attacks."

This was the message coming out of the 2018 NATO Brussels Summit declaration, and indeed, the current and foreseeable security landscape looks increasingly 'hybrid' in nature. Hybrid operations and tactics combine military and non-military as well as covert and overt means, including cyber-attacks, disinformation campaigns, use of irregular groups and regular armed forces, espionage, sabotage, economic pressure and personal coercion. The strategic aim of such activities is to blur the lines between peacetime, crisis and conflict – to sow doubt and to foment divisions.

This development calls for new ways of dealing with such threats as well as for putting special emphasis on increasing our overall resilience against hybrid attacks. Even if not all these tactics are entirely new, tackling them effectively demands a more 'horizontal' and comprehensive approach.

Responsibility for building resilience against, and responding to, hybrid attacks lies primarily with individual states. However, it is impossible to deal with the range of such threats alone. Given the multitude of domains and individuals potentially affected, as well as the cross-border nature of many hybrid activities, more cooperation is required at all levels.

This includes international organisations like NATO and the European Union, who play an increasingly important role in bringing together

different perspectives, knowledge and expertise. In 2016, the two organisations identified areas for strengthened cooperation, which now amount to 74 actionable points. These cover different areas that include countering hybrid threats, cyber defence, enhancing resilience, training and exercises. Aiming for complementarity and non-duplication, both organisations can provide support to nations targeted by hybrid attacks.

A large part of the hostile activities that we today define as 'hybrid' is carried out in and through cyberspace. As cyberattacks are becoming more frequent, complex, destructive and coercive, strengthening cyber defences is a top priority for NATO. The Alliance is prepared to defend its members against threats in cyberspace as well as on land, at sea or in the air. It continues to develop new capabilities, build capacities, share best practices and enhance information-sharing.

NATO Allies have re-affirmed that international law applies in cyberspace. The Alliance supports the work underway to maintain international peace and security in cyberspace, to promote stability and to reduce the risk of conflict. The international community stands to benefit from a norms-based, predictable and secure cyberspace.

Over the years, NATO's approach to cyber defence has developed in a measured and responsible way and in response to an evolving cyber landscape. At the Summit in July 2018, NATO leaders took the next steps in enhancing their defences in the cyber domain, recognising the contribution that it makes to NATO's broader deterrence and defence posture. They also agreed on how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, and to establish a new Cyberspace Operations Centre. Allies are determined to employ the full range of capabilities, including cyber, to deter, defend against and counter the full spectrum of cyber threats, including those conducted as part of a hybrid campaign. Allies re-committed to fulfilling the Cyber Defence Pledge, which in the two years since its adoption at the 2016 Warsaw Summit has seen all Allies bolster their own national cyber defences.

While the Alliance must be prepared to respond to cyber threats and attacks, it also welcomes efforts to help prevent them in the first place. Information is continuously exchanged between the cyber incident response teams of NATO and the EU. This is done through the Technical Arrangement on Cyber Defence, concluded in February 2016, which facilitates cooperation at the operational and tactical level.

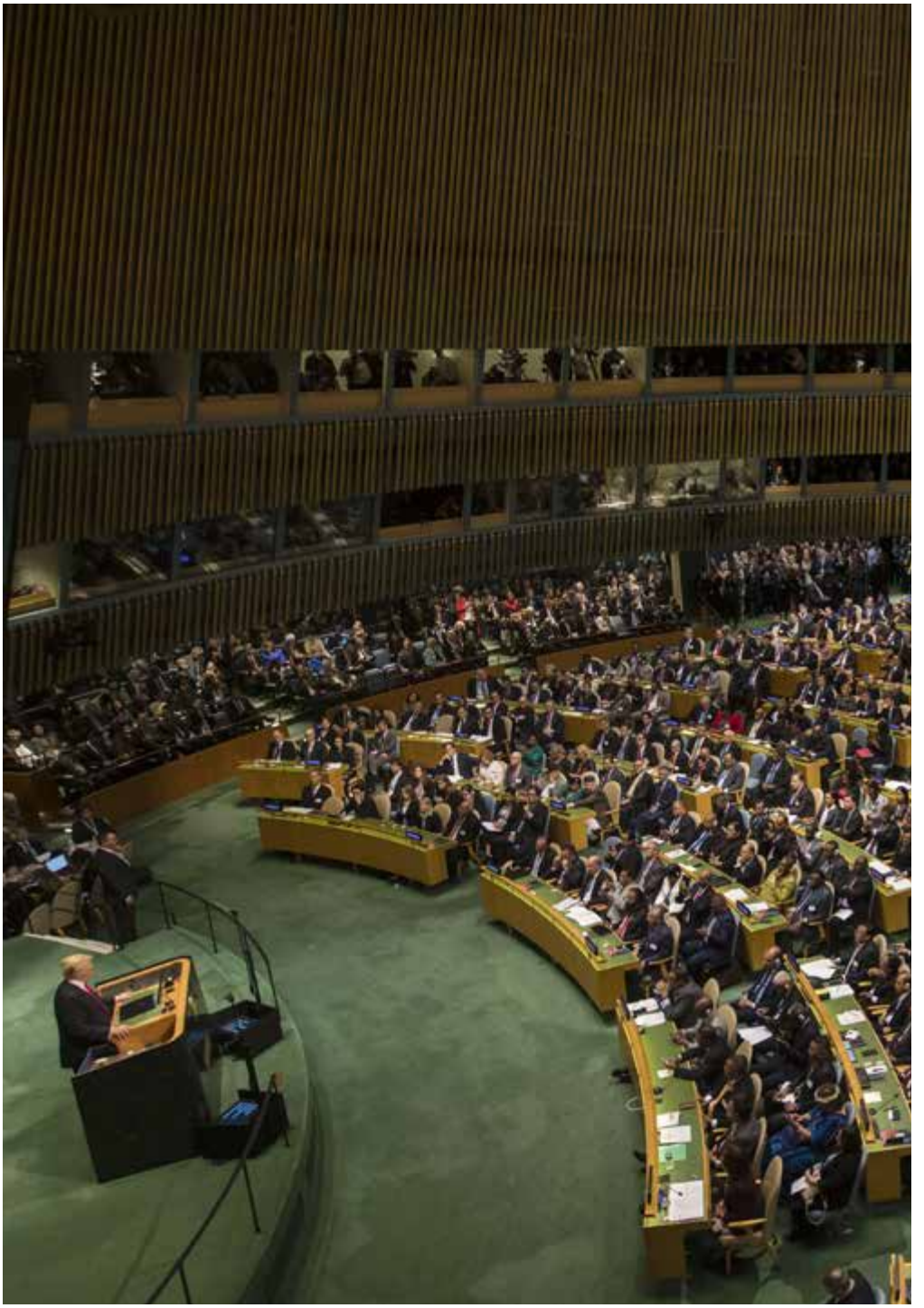
NATO is prepared to assist any Ally against hybrid threats, including through Counter Hybrid Support Teams – a new mechanism designed to improve active management of the response to hybrid threats. Under this new initiative, teams would support Allies' national efforts through tailored assistance if and as requested.

As policies and approaches continue to evolve, both NATO and the EU are paying more attention to how they are equipped to manage and

respond to potential crises. This is especially important because many cyber and hybrid activities fall below NATO's Article 5 threshold. In cases of hybrid warfare, however, the North Atlantic Council could decide to invoke this measure. This is also the case for cyberattacks, as their impact could be as harmful to modern societies as a conventional attack.

Both NATO and the EU have made significant progress in recent years to address rapidly evolving security challenges and to strengthen capabilities. Deepening cooperation between the two organisations makes a substantial contribution to preventing and responding to hybrid attacks.

Be it through information exchange, workshops or parallel and coordinated exercises like CYBRID, CMX, PACE or Cyber Coalition, the two organisations continue to ensure that by working in complementarity and avoiding duplication the overall resilience against hybrid attacks is being increased considerably. As recognised by both NATO and the EU in July 2018, this cooperation is essential in making the Euro-Atlantic area safer.



The need for international norms to help govern conduct in cyberspace

Governments alone cannot decide on all aspects of cyberspace

Marina Kaljurand, Chair of the Global Commission on the Stability of Cyberspace and Former Minister of Foreign Affairs of Estonia

In 2007, Estonia was the target of what some call the first strategic cyberattack in history. Over a three-week period, one of Europe's most wired nations was paralysed by a series of DDoS attacks against its government, media agencies and financial institutions. It marked a watershed moment in the use of state-sanctioned cyberattacks to advance foreign policy goals. It also introduced a model for conflict in cyberspace fought by proxy with the intention of retaining a degree of plausible deniability.

Conflicts between states are taking new forms, and cyberspace is likely to play a leading role in this newly volatile environment. Behind this backdrop lies the concern that a catastrophic cyber exchange between nation states could occur. In recent years, this threat has often been described as a major threat in national security threat assessments. These developments threaten to risk undermining the peaceful use of cyberspace and its potential role as a facilitator of economic growth and the expansion of individual freedoms. While this dire outlook is partially connected to the overall level of geopolitical tension, cyberspace is becoming an increasingly exploited resource that few feel compelled to take responsibility for, leading to a steady decay of the stability and security of the entire environment itself.

Both bilateral and multilateral interstate discussions have attempted, and in some cases have managed, to address some of the risks involved in inadvertent escalation as well as the loss of escalation control. The norm development principle was initiated in previous

years by the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). Already in 2013, this group agreed that international law is applicable in cyberspace and issued a set of norms of responsible state behaviour in peacetime. In total, the UN GGE process has issued 11 norms so far, some of which are fairly concrete. For instance, the 2015 UN GGE report stated that states should not "interfere with critical infrastructure", nor should they "conduct or knowingly support activity to harm the information systems of the authorized emergency response teams of another State. A State should neither use authorized emergency response teams to engage in malicious international activity."

Since then, however, consensus has eroded on how existing agreements and international law can and should be applied to this realm, given the complexity and increasing volatility of the environment in which they operate. Attempts to find a workable interstate dialogue seem to have reached an impasse. The failure of the UN GGE to reach a consensus in 2017 and stalemates in other diplomatic fora show that governments alone will not be able to fix the problem. Despite states' traditional dominance over all questions related to international peace and security, their role within the overall cyberspace ecosystem is limited. After all, the Internet is governed by a complex ecosystem of stakeholders, each with its own set of standards, norms, rules and processes. Governments alone cannot decide on all aspects of cyberspace – a space in which civil society writes much of the key code and the private sector owns nearly all the digital and physical assets. Given this complex landscape, it is unlikely that there can be a singularly encompassing legal solution that is both enforceable and inclusive. Instead, developing norms of behaviour acceptable to all relevant stakeholders is essential.

In industry and civil society, norms may be much more practical. These norms are usually based on technical best practices. MANRS (Mutually Agreed Norms for Routing Security) is just one such example that draws on a number of agreed-upon best practices known in the routing community. Norms are therefore not only at the end of a negotiation – such as in the UN GGE process – but they actually can be at the beginning as well. They can be a foundation that all can agree on and upon which further discussions can be based. Seen from this perspective, norms form a test of "what needs to be done" – a practical sense-test of what practical and operational steps need to be undertaken to achieve some measure of stability. They can be used to test our understanding of existing international law, or even more general principles, rather than the other way around.

This type of "bottom-up" process represents an important step towards defining and promoting responsible behaviour on the part of all parties involved, and this is why I believe that initiatives such as the Global Commission on the Stability of Cyberspace (GCSC) have such added value. In an effort to facilitate global multi-stakeholder engagement to help develop norms and policy initiatives related to international peace and

security in cyberspace, the Commission connects the traditional state-led dialogues with those of the Internet communities. It has focused its efforts so far on generating a set of additional norms specific to the most pressing issues today. But norms are not the end of the process. We must continue to be vigilant that already agreed norms are adhered to and that violations are monitored and called out. The question of how norms adherence can be best supported within the international security architecture will be a key focus of GCSC's work in the future.

This work is not undertaken in a vacuum. The GCSC is a civil society initiative and guided by significant, shared core beliefs, including the importance of a democratic, multi-stakeholder approach to governance. The cyberspace ecosystem is a highly complex arrangement with many different institutions, processes and regimes engaged in maintaining and working on (and in) cyberspace, all of them connected to each other in one way or another. Just as the norms drafted by diplomats can have relevance for technical actors in Silicon Valley, the best practices of the technical and Internet governance communities can be relevant for international security. Groups like the GCSC play a crucial role in translating between these various communities. Mutual coherence is not simply an option – it is a prerequisite for building cyber stability, for agreeing on what is good and bad behaviour in cyberspace, and, ultimately, what to do about it.

PART 2:
BUILDING RESILIENCE OF CRITICAL INFRASTRUCTURE: CASE STUDIES

Lessons from the Baltic States: strengthening EU resilience against Russian hybrid warfare

Hybrid warfare resilience relies on national and collective efforts

Eitvydas Bajarūnas, Ambassador-at-Large for Hybrid Threats, Ministry of Foreign Affairs, Lithuania

With Russia continuing to pursue an aggressive policy directed against the West, the Baltic States are often defined as a primary potential target of Russia's hybrid actions. For them, the term 'hybrid' has become relevant, not only at a theoretical but also at a practical level.

Over the past years, the Baltic States have been on the receiving end of Russia's advancements in the field of hybrid warfare. However, not only Baltic States have been affected by Russian malign operations. Russia is stricking right to the heart of our democratic way of life. Continuous agression in Eastern Ukraine and Syria; meddling into national elections and referendums, the latest of which took place in Macedonia; the poisoning of the Skripal family; supporting radical political parties; and provoking general confusion on decision-making in the West, to name just a few. These measures align with Russia's overall strategic goals to change the global power balance, to divide the transatlantic community, to dominate within its perceived zone of interests, including the Baltic Sea Region, and to sow ambiguity in order to exploit our weaknesses.

In the case of the Baltic States, Russia has long been using political and economic pressure as part of its aggressive policy against Lithuania and is particularly interested in the country's 2019 presidential elections. Most identified cyber activities in Lithuania are indeed tracable to Russian state actors, including hybrid and disinformation strategies targeted at NATO's Enhanced Forward Presence and aggressive campaigns making use of hostile information, historical as well as ideological policies to fuel the anti-Western sentiment of Lithuanians, or

exploiting ethnical tensions. Russia employs conspiracy theories, alternative truths and lobbying to discredit states in the international arena and harasses individuals who criticise the Kremlin. Russia continues its attempts to dominate the energy market of the Baltic region and to obstruct its integration into the Western European energy system. As an example, Belarus, together with the Russian corporation Rosatom, accelerated the construction of the Ostravets Nuclear Power Plant, failing to comply with the international nuclear security requirements.

So, how should a country like Lithuania respond to these ever-present and increasing threats?

First, a strong political mandate and a comprehensive security concept must be put in place. Robust political commitment from the highest level – president, prime minister, political elite – on the need to counter foreign influence and strenghen resilience is needed. Moreover, the Lithuanian National Security Strategy has implemented a comprehensive approach to security. Actionable points to address hybrid threats include establishing a system of coordination between the various institutions at governmental level and finalising crisis management mechanisms, using "the-whole-of-government" principle.

Second, key stakeholders must have a common understanding of the situation, a shared threat and risk assessment as well as planning and training processes put in place. Other actions included increasing the defence budget to exceed 2% of GDP, restoring the conscription system, territorial defence and rapid reactions units, and setting up regular exercises with EU/NATO counterparts. In response to cyber attacks, a cyber defence system was set up focusing on the protection of critical information infrastructure, the public sector, and increased resilience and response capabilities were put in place.

Third, Lithuania's efforts to counter disinformation were also outlined in the Security Strategy. This included strengthening strategic communications; raising public awareness of information wars and propaganda; and suspending propaganda of war and hatred. Providing social media literacy skills and other training to officials, politicians, the media and society has become an important issue in the fight against information threats. These educational endeavours are an active way to identify lies, deconstruct them and focus on developing the message and narratives on and of Lithuania. To this end, a group of independent fighters against propaganda, titled the 'Lithuanian Elves', was set up.

Hybrid warfare resilience relies not only on national efforts, but on collective ones as well. International cooperation, particularly through the EU and NATO, is crucial but concentrated initiatives such as the EU's East Stratcom Task Force, NATO's Counter Hybrid Support Teams, the European Centre of Excellence for Countering Hybrid Threats and Lithuanian-led PESCO initiative of Cyber Rapid Reaction Teams, among others, can also offer much to the fields of politics, strategy, cyber, economy

and military. This helps to "cover" some missing national capabilities and provide support in developing these competences that are not yet sufficiently developed at national level. International cooperation enables uniting separate, scattered national resources to better approach issues of a broader geopolitical agenda.

While the EU and NATO are making good strides in coordinating their activities, this is not yet enough. In addition to official meetings, multilateral initiatives and effective sanctions must be developed.

Some key policy conclusions can be drawn from the Baltic perspectives on the way ahead in countering Russian hybrid warfare.

While discussing hybrid threats and clarifying what they are is important, it is even more imperative to pursue concrete actions to fight these threats, both domestically and through multilateral actions, for example by "blacklisting" Russian diplomats. It is in the interests of the Baltic States to consistently inform Western partners about Russia's actions.

Appropriate instruments are also needed to successfully combat hybrid warfare. Coordination is very important, but it is not enough – the enemy is ingenious and has the advantage of the initiative, so the "old toolbox" will not always help. In all areas of security, bold actions and new tools are needed.

Unpredictability and uncertainty make hybrid threats more difficult to identify. Therefore, the elite and the media have the important, yet difficult, task to clarify these threats so that our societies remain vigilant and resilient. There is a need to support information pluralism, invest in civic awareness through education and maintain an independent press that responds swiftly to any disinformation.

Security experts and political leaders have an increased understanding of Russia's hybrid activities. However, this is not enough: we have to constantly seek for more information and exchange our experiences on the issue.

Hybrid defence is neither static nor conventional – we need to deepen our knowledge of new methods and tools in order to rise to the challenge.

Disinformation and fake news as the new normal: a challenge for the Western Balkans

Information provides the basis for an individual's understanding of reality

Tara Tepavac, Senior Researcher at the Center for Research, Transparency and Accountability (CRTA)

Disinformation and 'fake news' are nothing new – Yuval Noah Harari has even said that "Homo sapiens is a post-truth species, whose power depends on creating and believing fictions." As they keep growing and spreading with unprecedented speed in social and mainstream media, they have attracted considerable attention and have become a great cause for concern. A recent study conducted at the Massachusetts Institute of Technology found that false information and rumours spread "significantly farther, faster, deeper, and more broadly than the truth", and that it takes truth six times as long to reach 1,500 people as false content does.

Fake content and information is not just a concern for expert and policymakers, but also for citizens across Europe. A 2018 Eurobarometer survey brought to light the citizens' rising concerns across the European Union, with over 85% of Europeans considering them a problem for democracy. And this is justified, given the immense consequences misleading information can have in vulnerable and unconsolidated democracies in particular. According to the 2018 Media Literacy Index, the Western Balkansand Turkey occupy the lowest ranks among the 35 European countries, with Serbia and Montenegro marking further deterioration in scores in comparison to previous years...

The results of the Regional Media Monitoring analysis in Bosnia and Herzegovina, Montenegro, Macedonia and Serbia conducted by CRTA confirm this finding: a considerable percentage of news published in these four Western Balkan countries lack clear sources and citations and feature biased reporting, which are typical characteristics for disinformation and 'fake news'. The results revealed that one

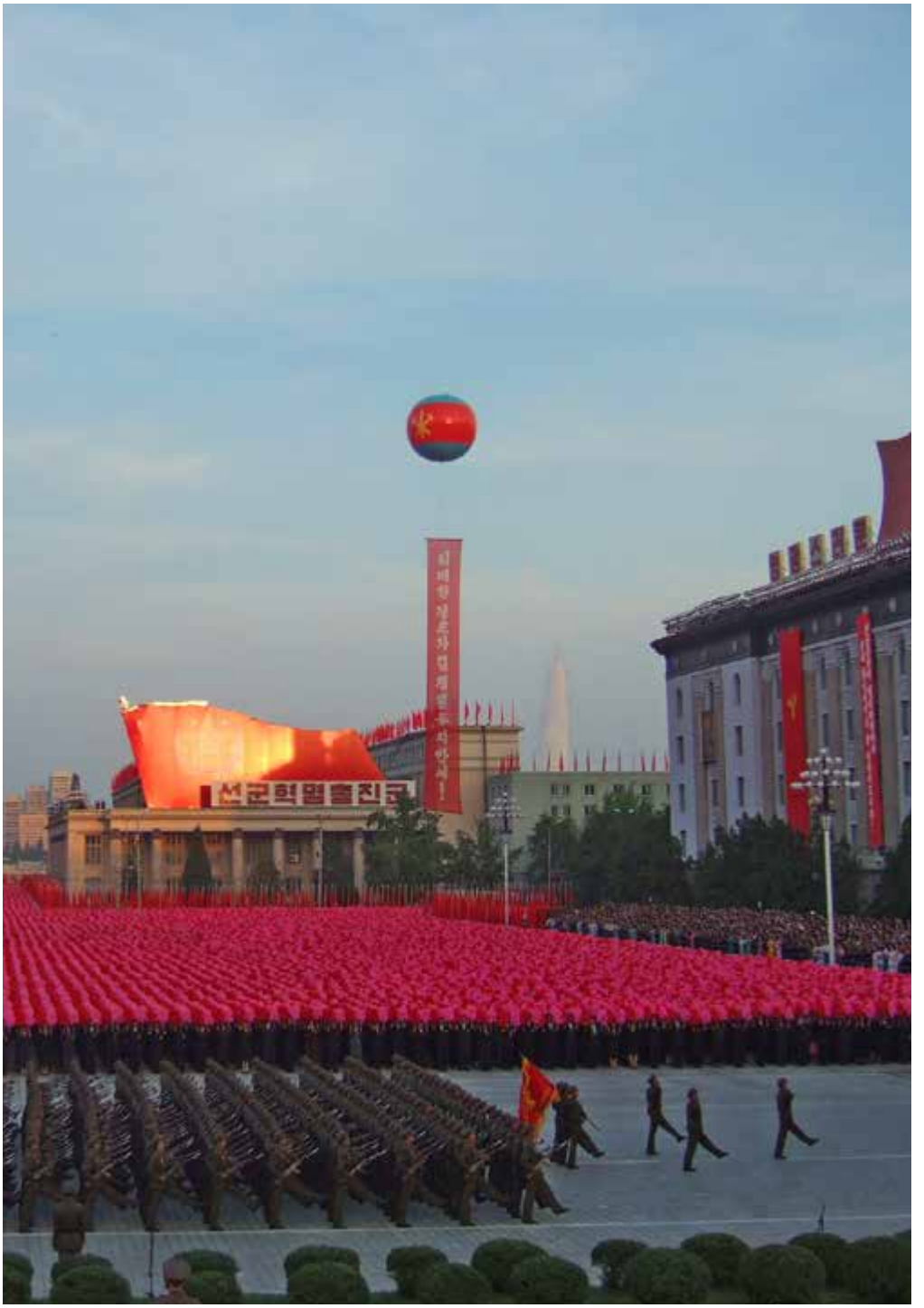
third of news and media reports in Serbia are without sources (i.e. with unknown authors), which mostly convey pro-Russian and anti-European or anti-American tones, while almost a half of pieces in Macedonia contain unnamed sources.

Media pieces and articles that lack sources or contain quotes from unnamed sources are particularly dangerous when they are focusing on topics related to politics or international affairs. For instance, media reporting in Serbia is predominantly positive towards Russia and predominantly neutral when it comes to the EU. Through this type of disinformation, the public opinion can be effectively influenced. CRTA's media monitoring of foreign relations in Serbia in 2017 demonstrates that politics and military affairs are the most frequent topics of articles featuring pro-Russian and anti-US discourse and that the majority of articles potentially containing fake news feature some kind of anti-Western position. In Serbia, Russia is often perceived to be one of the main supporters while only less than a quarter of citizens recognise the EU among country's biggest donors, although in reality it is the EU that provides the most support, closely followed by the United States and several individual European countries such as Germany and Sweden. Russia's public image in Serbia is also shaped by the regional editorial office of Russian state-owned news agency Sputnik, located in Belgrade, the influence of which should not be underestimated given its rich radio programme, free content and online presence. This type of one-sided reporting is unfortunately gaining considerable influence in shaping the public opinion.

Information provides the basis for an individual's understanding of reality, thus making it one of the essential elements of a functioning democracy. Media's role is crucial: citizens rely on information obtained through media channels in shaping their perceptions, positions and voting preferences, and it keeps the governments and elected representatives accountable for their promises and actions. Unfortunately, this crucial element of the democratic system is also increasingly fragile and needs to be protected. In addition to polarising societies and increasing the mistrust towards democratic institutions and stakeholder groups, disinformation contributes to the overall decay of trust.

In order to counter disinformation, numerous countries are experimenting in developing a comprehensive strategic approach. Government task forces are being formed, new regulations are being debated and new initiatives by tech companies are being launched. However, a comprehensive solution cannot be achieved without long-term support to fact-based, reliable media – combined with efficient and reliable fact-checking initiatives – and systemic support in raising media literacy of citizens through tailored training, particularly that of the younger generations. Educating citizens, empowering them to recognise fake news and rebuilding their trust in people, politicians, society and democratic systems is the key for getting ahead in building resilience to disinformation.

The views expressed are those of the author do not necessarily reflect the views of CRTA.


선군혁명총진군

Assessing North Korea's cyber threat

Until recently, the security threat posed by North Korea was primarily geopolitical

Jenny Jun, Doctoral candidate, Department of Political Science, Columbia University

Since the Korean War, North Korea and South Korea have been embroiled in an intense strategic rivalry. For many years, North Korea's alleged goal has been to reunify the Korean peninsula under its rule. However, by the 1980s, the military balance vis-à-vis South Korea had started to reverse and winning a conventional war on the peninsula had become unrealistic for North Korea. Furthermore, with the end of the Cold War in 1991, Russian and Chinese patronage to North Korea diminished while the US-ROK alliance deepened. This new strategic environment limited North Korea's ability to explicitly take what it wanted with physical force alone, and it was forced to come up with new ways and means to coerce the adversary. North Korea's chosen approach was to increasingly rely on asymmetric strategies and irregular operations, which included both the adoption of new capabilities – such as a nuclear and ballistic missile programme – as well as the use of otherwise conventional means in ways that exploit asymmetric advantages.

The reasons behind North Korea's success in becoming a cyber threat worth taking seriously are simple: while it might not be the most technically sophisticated player, other countries do not have many options to deter North Korea both inside and outside cyberspace, and this gives it a unique asymmetric advantage.

Policymakers often seek to deal with cyber threats by building what they call 'cyber deterrence', or the means of preventing an adversary state from launching a cyberattack on their systems and networks usually by issuing a threat that any cyberattack will instigate a devastating and even greater counter-attack. However, with North Korea the problem is that there are very few options

left for twisting its arm when it comes to cyberspace. North Korea is not very reliant on cyberspace for its military, political or commercial activities so there is very little for the international community to hold hostage that North Korea would consider strategically important or costly enough to dissuade the use of cyber capabilities.

US policymakers often refer to North Korea as a "land of lousy options" when it comes to the nuclear context as there are simply no good options for compelling the country to give up its nuclear weapons. Increasing economic sanctions will not likely add enough marginal costs or risks for the regime to collapse. Both South Korea and the US, one of the most connected states in the world, simply have much more to lose from a cyberattack than North Korea does.

This imbalance of power leads to two key implications.

First, North Korea, more so than other states, may feel encouraged by the perception that its adversaries lack credible means to retaliate against the cyberattacks it initiates. Victims of a North Korean cyberattack may try to shut off North Korea's tiny intranet or indict North Korean nationals involved in the attacks, but it is dubious whether such measures – other than their symbolic value – carry enough weight to deter an attack in the first place.

Second, investing in resiliency, instead of deterrence, may be a more effective response. Resiliency seeks to minimise a cyber attack's impact by building processes that allow one's own systems and networks to quickly and efficiently resume routine operations after an attempt. If resiliency measures are robust and made publicly known, it could signal to North Korea that its cyberattacks are unlikely to have the devastating effect it intended to have, discouraging it from wasting time and resources into planning such an attack in the first place.

Until recently, the security threat posed by North Korea was primarily geopolitical – its long strategic rivalry with South Korea meant that North Korea was mostly a concern to East Asia, and the US by extension, and possibly the Middle East on nuclear and missile technology proliferation. However, cyber operations now transcend many of the geographical constraints of coercive diplomacy and criminal networks. North Korea, despite having very little conventional capabilities for power projection, has been nonetheless able to conduct operations such as the cross-continental SONY hacking incident. Sophisticated cyber operations also utilise third party infrastructures in otherwise neutral states to enable offensive cyberattacks on other targets. These suggest that the absence of a strategic rivalry with North Korea is not a sufficient reason to ignore its emerging cyber capabilities.

One such area is cybercrime. At the moment, North Korea is engaging in state-sponsored cybercrime without geographic constraints. The WannaCry ransomware attack that hit the UK the hardest as well as a series of

bank heists exploiting the SWIFT system targeting banks in Vietnam and Bangladesh are prime examples of these tactics. In 2014, a hacker group – later identified as North Korean – tried to extort money from a South Korean company responsible for the country's civilian nuclear reactors. Since 2018, North Korea has added targeting cryptocurrency exchanges to its repertoire. Their attacks are consistently becoming more sophisticated and diversified, and they are a concern for policymakers around the world irrespective of their geographical proximity to North Korea.

In conclusion, it makes political, military, and financial sense for North Korea to continue investing in its cyber capabilities, and its behavior in the past few years provide evidence that it remains determined in doing so. According to a 2013 National Assembly testimony from the Director of National Intelligence Service, Kim Jong-Eun allegedly referred to the state's cyber capabilities as an "all-purpose sword." While current negotiations and an accompanying friendly atmosphere among North Korea, South Korea, and the U.S. may lead to a temporary restraint on destructive cyber operations that may derail the conversation, its cyber espionage and criminal components have persisted and do not show signs of stopping anytime soon.

PART 3:
MANAGING THE THREAT: FORESIGHT, CRISIS MANAGEMENT AND DAMAGE CONTROL

Deterring future cyberattacks
EU, NATO and international responses

Cyber is the ultimate team sport where the larger the network and the more diverse set of partnerships, the more successful you are likely to be

Jamie Shea, Senior Fellow at Friends of Europe and Former Deputy Assistant Secretary General for Emerging Security Challenges at NATO (2010-2018)

In its brief history to date, cyberspace has made us accustomed to dramatic events and ever more daring and sophisticated attacks across the Internet and our information technology networks.

Yet, even by this high standard, 2018 is turning out to be the most spectacular year thus far. This year has seen an unprecedented naming and shaming of Russia by intelligence agencies in the United States, United Kingdom, Netherlands, Germany, Estonia and Australia. In September 2018, the US announced its new National Cyber Strategy, which places fewer restraints on the use of offensive cyber operations to hit back at those attacking American targets. Soon after that, the US also announced its first publicised cyber retaliation against Russian hacker groups. Visiting NATO Headquarters, the US Defence Secretary Jim Mattis stated that the US was now willing to contribute its cyber capabilities to the Alliance as part of NATO's programme to use cyberspace as a domain of military operations. At the same time, the EU October Summit in Brussels discussed how to enlarge the European Union's toolbox of diplomatic and economic response options against cyberattacks.

But this news also comes with a negative side. The US Government Accounting Office released an alarming report claiming to have discovered critical cyber vulnerabilities in US weapon systems worth a total of $1.55 trillion. Bloomberg reported a story that China had implanted tiny microchips in motherboards used by US tech companies, such as Amazon and Apple, thereby endangering servers utilised by both the government and private sector actors in the US and beyond. As a timely demonstration that cyberattacks are not only state-on-state activities and that criminal hackers have not gone away, Facebook acknowledged a compromise to its software that exposed the data of hundreds of thousands of its customers. British Airways also admitted to a massive data breach of its online booking system. Just another month in cyberspace, you might think.

The US has looked at its 16 critical national infrastructures, such as power, air traffic control, transportation and water supplies. Following allegations of foreign interference in 2016, election machines have been added to this list. As most of this critical infrastructure is today owned and operated by the private sector, the US government has worked to increase voluntary information-sharing as well as to promote risk assessment models and industry standards for cyber security, sector by sector.

In 2017, the EU accelerated its efforts by updating its 2013 cyber security strategy. The EU Network and Information Security (NIS) Directive establishes compulsory standards for companies operating within the EU, imposing major penalties in the event of non-compliance. A Framework for Responding to Hybrid Threats has also been agreed on and, at the time of writing, the EU is reviewing its diplomatic toolbox to expand its response options. A CYBRID exercise was held for EU Defence Ministers in Estonia in the autumn of 2017 to test their crisis management skills in classifying, attributing and responding to fictitious but entirely realistic cyberattacks against EU maritime forces and an EU military headquarters. The EU has also stepped up its cooperation with NATO. A technical agreement between the EU's Computer Emergency Response Team (CERT-EU) and the NATO Computer Information Response Capability (NCIRC) has allowed for faster and better information exchange between both organisations during incidents such as the Wannacry and NotPetya cyberattacks. NATO and the EU are conducting tabletop exercises to harmonise their procedures and working cultures and are coordinating on hybrid warfare scenarios and responses.

NATO has also put cyber defence centre-stage. The US, the UK, France, Denmark and Estonia have all offered NATO access to their cyber capabilities and the Alliance has formulated a mechanism to enable these transfers to take place in crisis or conflict. Through training and exercises, the introduction of cyber targets into NATO's defence planning process and Smart Defence multinational projects, NATO continues to assist its individual member states to become more cyber resilient. Meanwhile, NATO's Cyber Defence Pledge, adopted at the

2016 Warsaw Summit, is proving invaluable in inducing Allies to spend more on improving their national cyber security. Establishing a network of cyber research and development centres, linked to an EU centre, could help in this regard.

Still, much remains to be done, and staying up with the curve of technological change and the increasing exploitation of cyber space for both good and bad requires constant effort. A number of key issues have to be addressed.

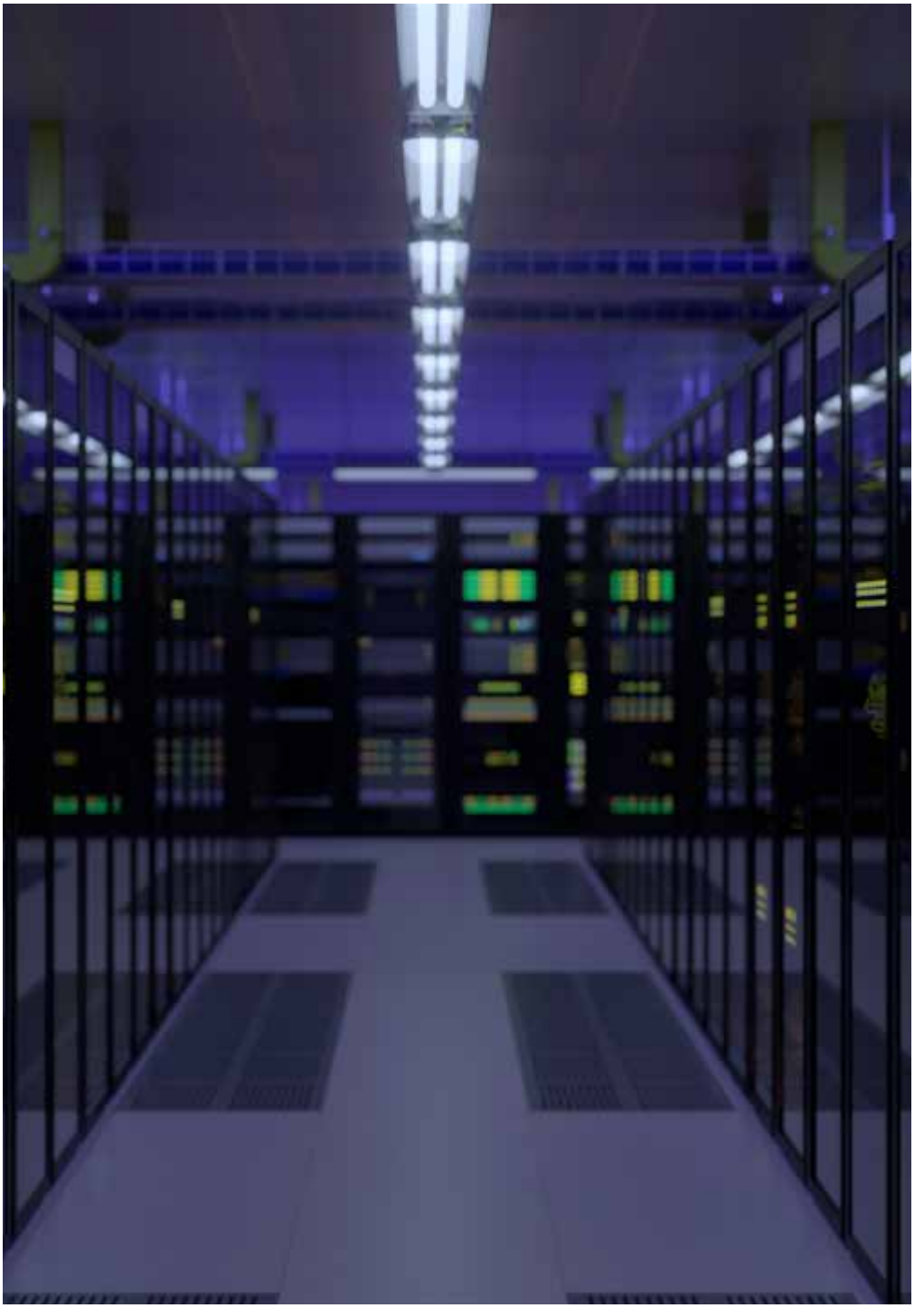
One is to develop more security by design so that new IT products incorporate protection as well as speed and connectivity.

Another is supply chain security: at a time when IT is the epitome of globalisation, there is a high risk of hardware and software hacking.

A third challenge is the cyber security of the civilian infrastructure as well as host nation support that NATO relies on for its military movements in Europe. This cannot become the Achilles' heel of the Alliance's deterrence and defence posture in Central and Eastern Europe.

Finally, how can we build the right eco-system to ensure that we do a better job of anticipating and adapting to our new world that is driven by data, by artificial intelligence, by the man-machine interface and by the growing role of virtual reality? This eco-system needs to address both the short-term threats and the longer-term challenge of building a secure, trusted and humane cyberspace that empowers individuals rather than enslaves them. It has to make politicians more knowledgeable about technology and science, better able to identify and promote new forms of global, or at least regional, governance through norms and codes of conduct. It also needs to be able to reach out to the private sector and civil society.

Cyber is the ultimate team sport where the larger the network and the more diverse set of partnerships, the more successful you are likely to be. It could be the first significant security challenge in history that is best handled bottom-up rather than top-down.



Hybrid threats need a hybrid response

Europe needs to get better at developing and promoting a compelling positive narrative

Giles Portman, Head of the East Stratcom Task Force at the European External Action Service

Disinformation has been with us since the Garden of Eden but it has recently become a key element of the hybrid warfare toolkit. Our decision-making processes are under threat from those who seek to undermine our open and democratic societies and interfere in our debates and electoral processes. Technological advances, such as artificial intelligence, are helping them reach millions of people in the blink of an eye. Meanwhile, scepticism towards mainstream media and politics creates an enabling environment for false messages and fake news to gain traction.

In June 2018, European leaders asked for a new action plan on disinformation, which will be presented to the December 2018 European Council. It will build on the pioneering work of the East Stratcom Task Force, which was set up by EU Heads of Government in 2015 to respond to Russia's ongoing disinformation campaigns.

The pro-Kremlin disinformation campaign seeks to divide and confuse us by weakening our consensus, exacerbating tensions and impeding effective decision-making. Whether the subject is the poisoning of the Skripals, the ongoing conflict in Syria or the shooting-down of civilian airliner MH17 over Ukraine, the campaign deploys a constant stream of partial, distorted or false narratives, the aim of which is not to inform but to disinform. The East Stratcom's weekly 'Disinformation Review' is a public resource that tracks, identifies and exposes these misleading and often contradictory narratives.

It is essential that we continue to catalogue the tools and techniques hybrid warfare practitioners utilise and continue to analyse the intentions of their campaigns. However, we also need to raise awareness of these campaigns – and of the European Union's response – through the 'EUvsDisinfo' initiative, which also

has a heavy presence on social media. At the same time, we must also evaluate the overall challenge external disinformation presents to Europe, assess the risks and incorporate the analysis of intelligence-based EU bodies like the Hybrid Fusion Cell.

But identifying and debunking false narratives alone will not restore confidence and trust. Europe needs to get better at developing and promoting a compelling positive narrative of what its policies seek to achieve and the concrete benefits they bring to citizens. The East Stratcom Task Force has led the way in this regard by developing a campaigning approach to EU communication in and about our eastern neighbourhood. As many citizens increasingly believe only what their friends and family tell them, we need to communicate with this level of granularity in mind, namely by using deep and local audience insights and examples; adopting a storytelling approach; focusing on tangible benefits gained not money spent; and seeking the help of trusted and authentic local multipliers to reach the audiences that are otherwise out of reach. The EU's communication task forces for the Western Balkans and the southern neighbourhood are implementing similar strategies.

The EU Action Plan launched in December will put all this work into a broader context, and it comes at a crucial point in time, given next year's European elections. For three years now, the East Stratcom has catalogued a pattern of misrepresentation and attempted interference in European electoral processes. In his 2018 State of the Union speech, President Jean-Claude Juncker stressed the urgent need to secure free and fair European elections in 2019 and announced a plan to counter the threats caused by disinformation campaigns and cyberattacks as well as by the lack of transparency and misuse of personal data.

Moreover, the European Commission issued its April 2018 Communication in a step to enhance the transparency, accountability and trustworthiness of online information. This has led to a new Code of Practice, signed in October, for social media platforms to commit to greater transparency over issues such as funding, sources and beneficiaries of political advertising. We need to ensure that the same standards we expect of traditional media also apply to the digital sphere.

Disinformation is neither linear nor easily predictable: we need to improve our detection and analytical capabilities and base our findings on comprehensive monitoring and gathering of data. This means investing both in the tools needed to detect the hostile narratives that are gaining momentum and in the experts needed to make sense of this information. However, this requires resources and investment if it is to be done properly.

We can also make better use of the best practices that are already out there. At the moment, there are examples of excellence across Europe but the whole is not greater than the sum of its parts. We need closer coordination between member states and EU institutions and need to identify and connect the experts in each country. We need to also

create a platform for sharing best practices and warnings of emerging threats. At government level, we need to develop new mechanisms to work with businesses, media and civil society and identify the actions needed in the short-, medium- and long-term. We also need to keep supporting quality, independent journalism.

Facing hybrid threats requires a hybrid response. This means identifying, deterring and disrupting actors sharing disinformation; improving the transparency and trustworthiness of the online environment; and increasing audience resilience through education in media literacy skills.

There's plenty of work to be done.

Communications Service Providers play a key role in fighting cyber attackers

All businesses have a duty to make sure that they are properly protecting their customer data

Mark Hughes, President of BT Security

Whether a question of stealing huge volumes of data, ransomware attacks that cripple the operations of global companies or state-sponsored aggression, cyberattacks have become almost everyday news. Recent research by BT Security found that 97% of large businesses have been a victim of a cyberattack but only 22% were fully prepared to deal with a future attack.

The question is: why do so many companies feel unprepared to deal with cyberattacks? From my experience, there are three key reasons.

First, the adoption of new and disruptive technologies such as the cloud, the Internet of Things and big data by large companies has brought great opportunities to achieve growth, increase productivity and cut costs. However, they have also made our digital environments more complicated and difficult to secure. For example, there are now more Internet breakout points, more devices connected to the network and more data and applications hosted by third party providers with security controls that are not directly controlled by their customers.

Second, cybercrime has become professionalised. Well-resourced criminal gangs work in partnership with nation states. Exploit kits, developed and sold by criminals, have made it much easier for those without technical knowledge to perpetrate cyberattacks which has led to a rise in the volume of attacks.

Third, there is a global shortage of skilled cybersecurity professionals. Our research has shown that 45% of companies lack the skills and people they need to defend themselves. Combine this with an increasingly active threat landscape and a more complex digital environment to secure and you can see why cybersecurity experts are struggling to keep up.

This is a complex problem which can only be solved by the private sector, in collaboration with national governments. Communications Service Providers (CSPs), such as BT, are in a unique position as they work closely with governments and law enforcement bodies due to their ownership of the telecommunications and Internet infrastructure, the global visibility on cyber threats and the expertise that is developed in defending business and customers against cyberattacks.

Last year, 250,000 cyberattacks were attempted against BT alone. A major part of the critical national infrastructure, we are a target for nation states, criminal groups, hacktivists and terrorist organisations. We also supply services to customers across a much wider range of critical infrastructure. Our network is relied on every day by the government, the military, banks, utility providers and transport enablers such as air traffic control and navigation systems. We have therefore developed the experience and expertise needed to defend our customers against the best-resourced and most determined attackers. We work closely with government agencies such as the National Cyber Security Centre and the National Crime Agency in the UK to offer both strategic and operational support for investigations.

Our need for skilled experts and our experience in training them make us a key partner for the government who is working hard to close the cyber skills gap. We recently published our plan to bridge the cyber skills gap in the United Kingdom and work closely with governments to raise awareness about the great career opportunities in cybersecurity, with a focus on young people in schools and at universities.

Owning the Internet infrastructure means that we are able to work in partnership with the UK government to make life harder for cyber criminals. Leading work in this area through the National Cyber Security Centre's Active Cyber Defence programme, we have, for example, contributed to strengthening the Border Gateway Protocol in order to make it more difficult for UK machines to participate in a distributed denial-of-service attack. We are also protecting customers by blocking access to online sites which are known to be infected with malware.

Our global infrastructure gives us an unrivalled view of the threat landscape. One terabyte of data passes through our network every second. Of this, we currently process 600,000 events per second (2.1 billion events an hour) into BT's Cyber Security Platform which enables us to proactively hunt threats in real time. We then share this information with government and law enforcement partners,

such as Interpol and Europol, and even with our competitors. Earlier this year we set up our Malware Information Sharing Platform to share malicious domains and threat indicators with other CSPs. Over 300,000 malicious domains have been shared so far.

In our view, all CSPs have the responsibility to make it as easy as possible for their customers, whether they are global enterprises or individual consumers, to use the Internet safely. This is why we build security into all our consumer products and services from the start, help people block malware and choose strong passwords. We have also helped the UK government to develop guidance on designing consumer products that are secure from the outset.

CSPs play a central role in working with governments to defend civil societies and infrastructure against cyberattacks. But this responsibility is not ours alone. All businesses no matter their size have a duty to make sure that they are properly protecting their customer data and providing products and services that are safe and secure to use online. It is only when we all accept this responsibility and work together that we have a fighting chance against cyber attackers.

EU response to pro-Kremlin propaganda needs a change of pace

No sophisticated threat can be countered by volunteers only

Jakub Janda, Director of the European Values Think-Tank and Head of the Kremlin Watch Program

Since the Russian invasion of Ukraine in 2014, massive disinformation campaigns have been launched within European countries to support Russia's aggressive military actions. The aim of these campaigns was simple: downplaying and relativising the fact that Russia had invaded another country by spreading lies claiming that there were no organised Russian troops operating on Ukrainian soil.

Given the high volume of pro-Kremlin disinformation, in March 2015, the European Council gave a declaration according to which this type of disinformation is to be considered and addressed as a national security threat. Later that same year, the High Representative for Foreign Affairs and Security Policy, Federica Mogherini, was tasked with launching a team of expert specialists on this new threat. In autumn 2015, the East StratCom Task Force, consisting of around a dozen specialists nominated by the EU member states, launched its regular communication called Disinformation Review. The idea behind it is simple but powerful: dozens of volunteer specialists from journalists to security analysts – each of them knowledgeable of their national linguistic and political landscape – focus on mapping and exposing pro-Kremlin disinformation. More than 4,000 cases have been reported, debunked, and analysed since late 2015.

One would expect that if such a major threat was presented to and recognised by the EU leaders, the EU institutions would dedicate significant resources to ensure its smooth operation. Despite the many EU foreign ministers that have decided to support the Task Force; the European Parliament's allocation of €1m to fund 16 additional staff members; the fact that hundreds of European security experts have called publicly for this team to get any real

funding – the result to date is zero. Three years since the launch of the Task Force, several hundred volunteer specialists across Europe are still doing this highly needed job for free. But no sophisticated threat can be countered by volunteers only, even when they receive the support of around a dozen experts paid by the European External Action Service (EEAS). The EU currently spends more money on security guards in the Commission buildings than it does on countering pro-Kremlin disinformation.

In response to the wide criticism of doing too little, the Commission decided to go around the problem. Instead of using existing expertise and hundreds of available specialist assessments, it launched the 'High Level Expert Group on Fake News'. Consisting of 39 individuals allegedly representing the expert community, none has been a regular contributor to the work of the only EU body tackling this issue, the East StratCom Task Force, and no key European expert NGOs or think-tanks, who have been working on this area since 2015, were involved either, despite the EU's argument of bringing in civil society and NGO volunteers being key to this effort. The High Level Group's final report features a clear, undeclared objective: to downplay the fact that the main adversaries, creators and disseminators of hostile disinformation in Europe are Russia and its proxies.

However, the East StratCom Task Force still lacks budget for specialised research on this complex topic, and daily operational analysis of disinformation cannot be done because of the lack of in-house specialists. Since 2015, numerous appeals by the European Parliament, Foreign Ministers from the member states and dozens of European security experts have made the case why the East StratCom Task Force needs to be given resources – otherwise the EU will keep losing the battle in this area. In late 2018, three years after the only European Council-mandated EU specialist team was launched, it is still trying to survive inside the EEAS structure, while it should be leading the EU institutions in this area. The East StratCom needs deeper political commitment and more investments in the human and financial resources necessary to practically counter pro-Kremlin disinformation. As it currently stands, not enough has happened at the EEAS.

Other institutions and actors have tried to compensate this lack of response by the EEAS: Directorate-General for Neighbourhood Policy and Enlargement Negotiations (DG NEAR) funds activities in the EU's neighbouring regions, Directorate-General for Communications Networks, Content and Technology (DG CONNECT) plans to unveil a code of conduct for social media and several member states have taken this threat very seriously, taking action at national or regional level.

One can only hope that positive developments on this issue will take place in the aftermath of the 2019 EU elections.

Image credits:

Cover: shutter2u / Bigstock

p.8: GSshot / Bigstock

p.12: Rawpixel.com / Bigstock

p.15: bjginny / Bigstock

p.16: jaroslavav / Bigstock

p.19: Belish / BigStock

p.20: palinchak / BigStock

p.24: goncharovaia / BigStock

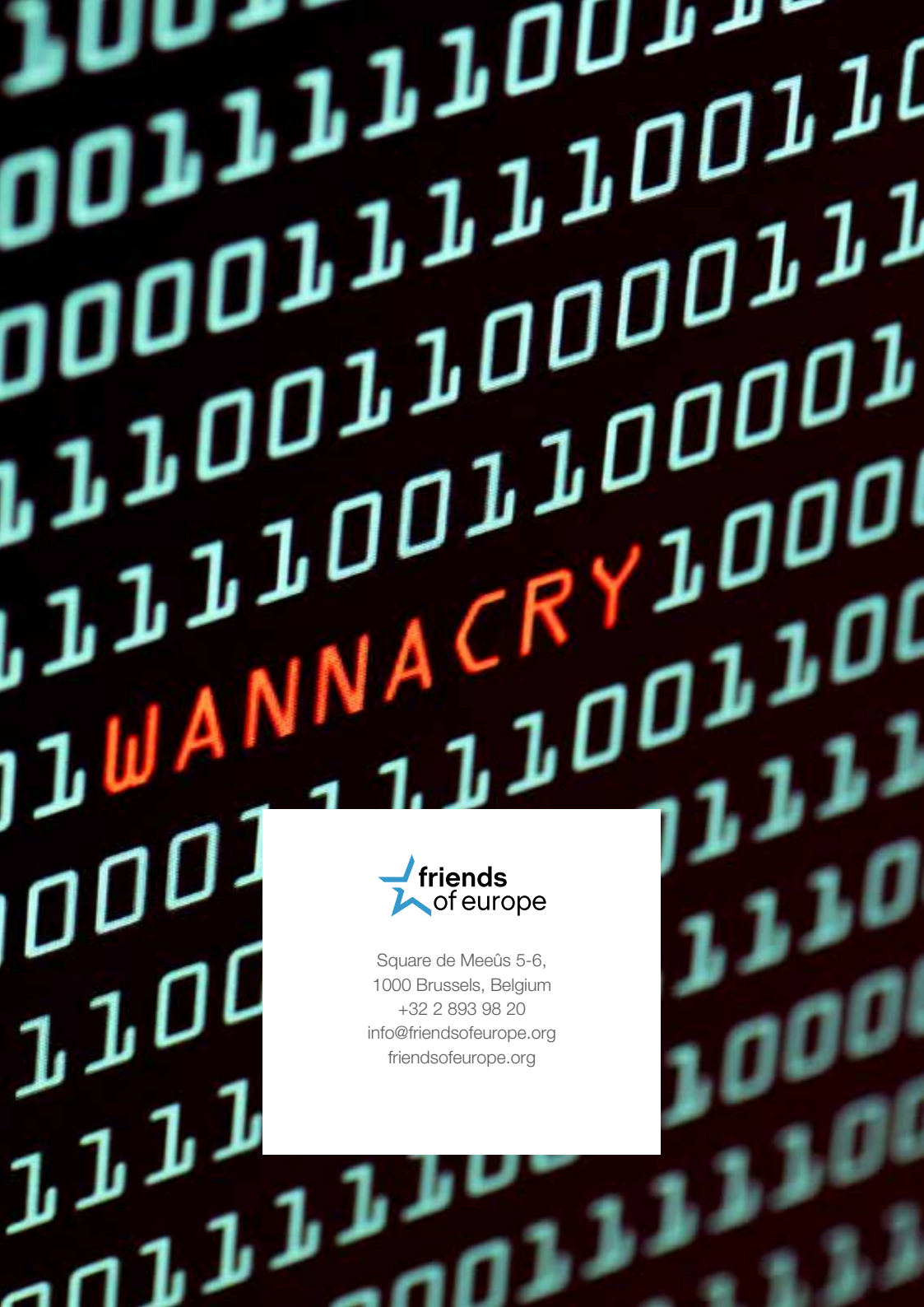
p.30: tupikov / BigStock

p.34: Studio37 / BigStock

p.38: toxawww / BigStock

p:42: David Franklin Studio / BigStock

This report is printed on responsibly-produced paper



friends of europe

Square de Meeûs 5-6,
1000 Brussels, Belgium
+32 2 893 98 20
info@friendsofeurope.org
friendsofeurope.org