No 2018/06, February 2018

EU Cybersecurity and the Paradox of Progress

Lorenzo Pupillo

Summary

Technological revolutions bring opportunities, but sometimes even greater threats. This 'paradox of progress' affects cyberspace today, threatening to undermine the very principle and foundation of the open internet. The global debate on cyber-governance is currently in a stalemate on the norms for global stability of cyberspace and the fight against cybercrime, although the EU is making considerable efforts to strengthen the resilience of cyberspace and the critical information infrastructure. The newly proposed Cybersecurity Act should, however, be supported by additional measures to increase awareness, devise smarter policy and enable effective governance. Too many users and businesses are still failing to take cybersecurity and computer hygiene seriously. And there is a need to strengthen the pan-European coordination of deterrence, detection, and defence. This paper looks at the possibilities for the EU in this domain and argues that at a time of American diplomatic and political retrenchment from Europe and the world, it has an opportunity to play a leading role in global cybersecurity policy and governance.

Lorenzo Pupillo is Associate Senior Research Fellow at CEPS and Head of the Cybersecurity@CEPS Initiative.

978-94-6138-670-0
Available for free downloading from the CEPS website (www.ceps.eu)

Contents

EU Cybersecurity and the Paradox of Progress

Lorenzo Pupillo

CEPS Policy Insight No. 2018-06 / February 2018

Introduction

Cybersecurity is the talk of the town. It is invoked with a sense of urgency in the most important political fora around the world. Many citizens have now become familiar with the arcane names of cyberattacks such as WannaCry, Petya and, more recently, Meltdown and Spectre, two of the worst IT security failures ever seen. To many companies, the question is not whether, but when they will be hit by a cyberattack. According to some observers, this is a sign of the times: the nature of global conflicts is changing profoundly. The US National Intelligence Council Global Trends Report warned recently that

> future conflicts will increasingly emphasize the disruption of critical infrastructure, societal cohesion, and basic governments functions in order to secure psychological and geopolitical advantages, rather than the defeat of enemy forces on the battlefield through traditional military means.[1]

At a time when we rely increasingly on the digital infrastructure for the storage of data and the delivery of key services, those same assets become the main, and probably easy, target of cyberwarfare: this is the so-called paradox of progress; our society is more efficient as digitalisation progresses, but is also more fragile.

This is the so-called paradox of progress; our society is more efficient as digitalisation progresses, but is also more fragile.

The new age of cyberwarfare is characterised by a rise in state-sponsored cyber offensives. These include, among others, *collection operations*, such as Russia's attacks on the networks of the US Democratic Party in 2016, or recent attempts to influence European elections, mostly to stir up social unrest and destabilisation; and *intrusions to hold targets at risk*, i.e. network intrusions to develop offensive capabilities against future targets, such as the attack on the power grid in Ukraine in 2015 or, possibly, North Korea's involvement in the WannaCry ransomware of last year.[2] These offensives are likely to succeed: offence has plenty of options when it comes to penetrating networks and data centres, whereas incentives to invest in cybersecurity are insufficient in an interconnected society in which only a collective and coordinated effort between private and public players can lead to sufficient levels of resilience. In other words, attackers only have to be patient: they will, sooner or later, hit the

[1] US National Intelligence Council (2017), "Global Trends: Paradox of Progress", January, p. 20.

[2] Ben Buchanan and Michael Sulmeyer (2016), "Russia and Cyber Operations: Challenges and Opportunities for the Next U.S. Administration", Carnegie Endowment for International Peace. See also David E. Sanger (2017), "U.S. Accuses North Korea of Mounting WannaCry Cyberattack", *The New York Times*, 18 December.

target. These reiterated attacks make cybersecurity a permanent, 24/7 activity; accordingly, the line between 'peacetime' and 'wartime' is blurred, as warfare is 'softwarised' and made constant.

'Resilience' requires not only world-class infrastructure, but also smart policies on preparedness, awareness and mitigation, as well as investment in enhanced awareness, smart policies and effective governance.

Will these trends permanently undermine security, or is there a way to build long-term opportunities? The buzzword here is 'resilience', which requires not only world-class infrastructure, but also a set of smart policies on preparedness, awareness and mitigation, as well as investment in enhanced awareness, smart policies and effective governance.

Enhance awareness: cybersecurity as a collective responsibility

One often-overlooked aspect of the WannaCry attack is that, even though more than 400,000 computers in over 150 countries were hit, millions were *not* affected because they had updated their software. For this reason, WannaCry was defined as a "tribute to negligence".[3] This is a common feature in modern cyberattacks: in most cases, basic computer hygiene such as keeping software updated, using strong passwords, encrypting sensitive data and keeping copies in the cloud are sufficient to protect computers from such incidents.[4] As mentioned in the 2017 High Level Group of Scientific Advisors on Cybersecurity to the European Commission,[5] many Europeans still fail to take basic cybersecurity measures: many say they care a lot about their personal data, but then give them away for free on social networks. Data are striking: 90% of the data breaches reported by the 2017 Verizon Data Breach Investigation were the result of phishing. And for those who are successfully phished it is not over because they can expect it to happen again at least once during the same year. Even some professionals do not take security issues seriously: in 2016 the Ponemon Institute revealed that 50% of interviewed professionals said that they had no password, PIN or biometric security guarding their devices, and two-thirds said that they didn't encrypt their data.[6]

Basic computer hygiene such as keeping software updated, using strong passwords, encrypting sensitive data and keeping copies in the cloud are sufficient to protect computers from such incidents.

Cybersecurity should therefore become a collective responsibility and cyber awareness and computer hygiene should become an integral part of digital literacy programmes.

Cybersecurity should therefore become a collective responsibility and cyber awareness and computer hygiene should become an integral part of digital literacy programmes. Without awareness-raising campaigns and smart policies, cybersecurity will always be dogged by collective action

[3] James Luiss (2017), Darwin and Ransomware, CSIS.

[4] See Roger A. Grimes (2018), "The two most imporatnt ways to defend aginst security threats", CSO, 7 February.

[5] European Commission (2017), "Cybersecurity in the European Digital Single Market", March, p. 21.

[6] J.R. Raphael (2017), "5 mobile security threats you should take seriously in 2018", CSO, 13 December.

problems, which trigger insufficient investment due to the likelihood of free riding. Put differently, computer hygiene and basic cybersecurity arrangements should become part of the everyday skills of any internet user, and in the corporate environment cybersecurity should become an overall management challenge, requiring a holistic risk- management approach. These issues seem to be on the radar screen of the European Commission, but a greater effort is needed to promote awareness in member states.

Smart policies for resilience

The EU launched its first initiative on IT security in 2006, later replaced by a Cybersecurity Strategy in 2013, and most recently by a comprehensive cybersecurity package in September 2017.[7] The latter includes far-reaching measures such as strengthening the role of the European Union Agency for Network and Information Security (ENISA); improving rapid emergency response to cyber-attacks; creating a Cybersecurity Emergency Respond Fund; building a cybersecurity competence network with a European Cybersecurity Research and Competence Centre; creating an effective criminal law response and increasing cyber defence capabilities. All these measures represent an ambitious plan and a significant step forward. However, given the very fragmented nature of the cybersecurity landscape in Europe and the voluntary nature of cooperation and information-sharing among member states, the EU's ability to operate through a single coordination point remains uncertain, at best. The need to build a European cyber shield might require a more federalist, not merely inter-governmental, solution, with one single EU body in charge of attributing responsibility to react and coordinate emergency responses to be implemented at the national level.[8]

... the fragmented nature of cybersecurity in Europe and the voluntary nature of cooperation and information-sharing among member states makes the EU's ability to operate through a single coordination point uncertain, at best.

In this respect, trust and coordination are the two pillars of a future EU cybersecurity strategy. Trust is not only needed between public institutions, but also between public and private players. Take, for example, information-sharing practices on data breaches. The cost of disclosing a breach can be significant and private, while the benefits of improved disclosure are pervasive and public. The imbalance between costs (sustained by a firm) and benefits (for all) generates a market failure. It is thus clear that new conceptual approaches to cybersecurity are required to make the behaviour of all players in this market more incentive-compatible.

In this context, it would be helpful to discuss the use of legal liability and insurance to create better incentives for safer behaviour and to work towards convergence between security and safety, especially in light of the emergence of the Internet of Things, which will embed

[7] European Commission (2017), https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en.

[8] See on this also EPSC (2017), "Building an Effective European Cyber Shield", Issue 24 May.

computer and communications everywhere.[9] Software will be omnipresent, but software and software-based products have inherent vulnerabilities. It has been estimated that the average programme has at least 14 separate points of vulnerability.[10] Each of these weaknesses could allow attackers to compromise the integrity of the product and potentially make an illicit entry. Software vulnerabilities therefore pose a serious concern for everyone and require the development of ad hoc policies to coordinate the disclosure of vulnerabilities and the implementations of the appropriate remedies coordinated vulnerability disclosure (CVD). At the moment, only few EU member states have these policies in place. Therefore, the role and the implementation of a CVD process across member states and precisely how and whether governments decide to release or retain a zero-day vulnerability for national security purposes (Vulnerability Equity Process, VEP) should be more broadly discussed to define a comprehensive framework to manage vulnerabilities. CEPS has promoted a Task Force on these issues and is working with the private sector, the EU institutions and civil society to suggest guidelines and recommendations for a CVD and VEP in Europe.[11]

Investing in relationships for a safer and more stable cyberspace

Trust-based relationships are essential to cybersecurity and resilience policy. A public-private, well-designed governance of emerging challenges such as massive, pervasive state-sponsored cyberattacks is becoming unavoidable. Yet global dialogue on these matters is not proceeding smoothly. Discussions about the introduction of global norms of responsible state behaviour, in particular the activity of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), are stalled on key issues such as the right of self-defence and state responsibility for cyberspace.[12] Likewise, only 56 countries have so far ratified the Budapest Convention on Cybercrime, 16 years after its official adoption.[13] At this rate, it would take until 2040 to have the majority of the world's nations sign it. Russia does not agree with Art. 32 of the Convention concerning trans-border access to stored computer data – and is proposing another treaty based on the Minsk Convention.[14] China, India and Brazil refuse to sign it since they were not involved in the negotiation and see the Convention as a

[9] See Eireann Leverett, Richard Clayton and Ross Anderson (2017), "Standardization and Certification of the "Internet of Things", mimeo.

[10] "The myth of cyber-security", *The Economist,* 8 April 2017, p. 9.

[11] See https://www.ceps.eu/content/software-vulnerability-disclosure-europe.

[12] Digital Watch Newsletter (2017), issue 22, 30 June (https://dig.watch/DWnewsletter22).

[13] Council of Europe (2018), https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Iua5Qg9O.

[14] See Wolfgang Kleinwachter (2018), "Internet Governance Outlook 2018: Preparing for Cyberwar or Promoting Cyber Detente?", CircleID, 6 January. The Minsk Convention on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters was signed in 1993 and is in force between the following states: Armenia, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russian Federation, Turkmenistan, Tajikistan, Ukraine, Uzbekistan. The Convention sets the rules for legal cooperation between member states' courts in civil, family and criminal matters. See CIS arbitration Forum (http://www.cisarbitration.com/about-cis-arbitration-forum/)

"fait accompli being forced upon them".[15] And today, the process is further hampered by frictions in Trans-Atlantic relations, which seem to be exacerbated by the Trump presidency and the agreement on permanent structured cooperation (PESCO) among 25 EU member states, raising questions about the future prominence of NATO.[16]

How are EU member states responding to these challenges? This situation has required them to use all the diplomatic and economic means at their disposal. First, the EU has developed a framework known as the Joint EU Diplomatic Response to Malicious Cyber Activities (the 'cyber diplomacy toolbox') that sets out measures under the Common Foreign and Security Policy, including restrictive measures such as sanctions.[17] Second, the new Cybersecurity Act proposed by the Commission aims to strengthen international cooperation on cybersecurity through the development of initiatives on external relations (bilateral, regional, multi stakeholder and multilateral engagements), the promotion of international cybersecurity capacity-building in third countries with a dedicated EU Cyber Capacity Building Network and increasing EU-NATO cooperation on cybersecurity. These measures are important but not sufficient to allow the EU to play a greater role in the international cybersecurity policy arena, especially considering the current geopolitical landscape and the potential role that a 'post-American Europe' could play in it.[18] Indeed, over the last decade, the US has reduced its diplomatic and political presence in Europe, creating an opportunity for Europe to take a greater responsibility in the international policy arena. Meanwhile, worried about the stalemate in international negotiations on confidence-building measures in cyberspace, the private sector has put forward specific proposals. Microsoft launched the idea of a *Digital Geneva Convention,* envisaging initiatives such as the no targeting of tech companies, the private sector or critical infrastructure and the creation of an independent organisation to investigate the attribution of nation state attacks to specific countries, like the role played by the Atomic Energy Agency.

Multistakeholder organisations such as the Global Commission on Stability in Cyberspace (GCSC) recently launched a *Call to protect the public core of the Internet,*[19] which is an appeal for a new set of rules for state and non-state actors mandating that they refrain from activity that "intentionally and substantially damages the general availability or integrity of the Internet itself".[20]

---

[15] See Rich Baich (2017), "International Cybersecurity Strategy", CSIS Report, p. 66.

[16] See Matthew Karnitschnig (2018), "Transatlantic tensions spill into view at security gathering", *Politico*, 16 February (https://www.politico.eu/article/defense-europe-transatlantic-tensions-spill-into-view-at-security-gathering/).

[17] European Commission (2018), https://ec.europa.eu/digital-single-market/en/cyber-security.

[18] Thomas Wright (2017), "A Post-American Europe and the Future of U.S. Strategy", Brookings Institution, December.

[19] GCSC (2017), https://cyberstability.org/wp-content/uploads/2017/11/call-to-protect-the-public-core-of-the-internet.pdf.

[20] Idem.

Against this background, the EU as 'norm superpower' should take the lead in this effort to define new norms to protect the civilian use of the internet and avoid its militarisation.

Against this background, the EU as 'norm superpower' should take the lead in this effort to define new norms to protect the civilian use of the internet and avoid its militarisation. Regarding cybercrime, the Budapest Convention is an important step, but it will only work if everyone adopts it. The current stalemate in the signature process of the Convention calls for new negotiating vehicles that would give to nations that do not agree with the text the opportunity to voice their concerns. Furthermore, the EU should increase bilateral activity and cooperation on cyber-security with 'fence-sitter' states such India and Brazil, still at the early stage of policy development, to move forward in the fight against cybercrime.[21]

Conclusions

Technological progress often comes with great opportunities, but equally important threats. The paradox of progress, already observed in medical research, has reached cyberspace. And if nothing is done to address it, it might critically undermine the very foundations of the open internet society. The EU's current efforts to create resilience and enhance deterrence in cyberspace are steps in the right direction, but critical issues still need to be addressed. The new Cybersecurity Act could represent an important opportunity, if accompanied by additional measures to increase awareness, smarter policy and effective governance. Too many users and businesses still fail to take cybersecurity and computer hygiene seriously. Greater effort is required to strengthen the pan-European coordination of deterrence, detection, and defence. And the international debate should shift gear with a more proactive European role in the definitions of new norms to protect civilians online and in the promotion of new initiatives to speed up the ratification of the Budapest Convention.

The diplomatic and political retrenchment of the USA from Europe and other parts of the world presents the post-America Europe with an opportunity to play a new role in much-needed global cybersecurity policy. Enhanced cooperation on security and defence among member states could mark a new era in the Union's involvement in global cyber-governance. Will EU leaders take up the challenge?

Enhanced cooperation on security and defence among member states could mark a new era in the Union's involvement in global cyber-governance. Will EU leaders take up the challenge?

[21] See Rich Baich (2017) and Thomas Renard (2018), "EU Cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain", European Politics and Society, 29 January.