COMMENTARY

Virtual Neighbors: Russia and the EU in Cyberspace

ANDRÉ BARRINHA*

ABSTRACT *The last decade has witnessed the consolidation of the European Union as a cybersecurity actor. Many of these developments have, directly or indirectly, been a response to Russia's activities in cyberspace. This commentary will explore and analyze the development of the EU's cyber actorness and assess whether it can effectively deal with Moscow's aggressive stance in this field.*

Introduction

The European Union (EU) is fast emerging as a central cybersecurity actor in international relations. The last few years have witnessed the development of a raft of legislation, communications and strategic documents that deal directly with this field. Much of this activism comes in response to Russia's cyberspace activities. That means that not only the EU is often placed in a reactive position, but also member states are often divided on how to engage with Moscow. As will be argued in this commentary, when it comes to cyberspace, Russia needs to be approached from three (albeit inter-related) distinct angles: as a cyber-crime hub, as a regional neighbor and as an emerging power, each of which demands a set of different answers, that range from deterrence to selective engagement. Only a multifaceted approach that includes, but goes beyond the EU's understanding of cybersecurity, can offer the possibility of an effective engagement with Moscow.

In terms of structure, this commentary will start by offering an overview of the EU's activities in cyberspace, followed by an assessment of how Russia fits into the EU's overall approach to cybersecurity and cyber diplomacy. The final part of the commentary explores the different ways

* University of Bath, UK

Insight Turkey
Vol. 20 / No. 3 / 2018, pp. 29-41

DOI: 10.25253/99.2018203.02

Nowadays, the EU also maintains cyber dialogues with Japan, South Korea and India and cyber is being integrated into enlargement and neighborhood relations, as is the case of the Western Balkans

in which the EU can deal with Russia when it comes to cyberspace.

Protecting the Digital: The EU in Cyberspace

The EU's approach to cybersecurity gained momentum[1] over a decade ago with the creation and development of a series of institutions, policies and initiatives that addressed the protection of critical information and cybercrime.[2] Surprisingly, however, cyberspace was to be absent from the 2003 European Security Strategy, in a clear indication that cybersecurity was not a security priority for the EU at the time. That would change in the following years, with the EU approving a number of relevant documents, including the 2006 EU Strategy for a Secure Information Society.

In 2008, cybersecurity was included –even if only briefly– amongst the global challenges and key threats of the Report on the Implementation of the European Security Strategy, which was an all-but-in-name revised security strategy. The motivation was clear even if not directly acknowledged: Estonia. In 2007, the Baltic country was at the receiving end of a series of cyber-attacks that severely impacted on the normal functioning of this highly digitalized society, with attacks targeting banks, government websites and other services.[3] The attack, attributed to Russian hackers, was not particularly sophisticated but the message was clear: information warfare was a real possibility,[4] and Russia was a reason for concern in this field. In April 2008, Georgia engaged in a limited confrontation with Russia over the territories of South Ossetia and Abkhazia. According to the Tbilisi authorities, the Russian offensive includes cyber-attacks similar to the Estonian ones, which included the defacement of governmental websites and distributed denial of service attacks.[5] These two cyber-conflicts would be taken into full consideration in the 2008 implementation report.[6]

More measures followed since, but it would take five years for the EU to have its first cybersecurity strategy. Eventually, in January 2013, DG Home Affairs Commissioner, Cecilia Malmström, High-Representative, Catherine Ashton, and DG Connect Commissioner, Neelie Kroes, drafted a rather encompassing strategic document that approached cybersecurity[7] from three main pillars of action: network and information security, law enforcement, and defense, each with its own set of policy priorities and institutions, such as the European Network and Information Security Agency (ENISA) and Europol's

European leaders pose during the launch of the Permanent Structured Cooperation (PESCO), in which 2 of its 17 projects are explicitly dedicated to cyber defense.

Getty Images

European Cybercrime Centre (EC3). In addition to the cybersecurity strategy, the EU approved a directive on attacks against information systems,[8] and presented a proposal for a directive on security of network and information systems (the so-called NIS Directive), which came into force very recently, and can be seen as the first concrete piece of EU legislation on cybersecurity.[9]

In terms of the international dimension of cyberspace, in November 2014, the EU approved the Cyber Defense Policy Framework, which addresses the global focus of the EU's activities in this field, with a particular concern for CSDP operations and relations with NATO. A few months later, in February 2015, the Council would approve some additional guidelines on EU cyber diplomacy[10] in order to promote a common approach and to more clearly define the role of the European External Action Service (EEAS) in this regard. In reality, at the time EEAS was only giving its first steps and the investment in cyber was limited, with no more than a handful of *fonctionnaires* dedicated to cyber-related tasks.

During this period, the EU started to consistently include a cyber-component in its bilateral relations with strategic partners. Until then, the main exception was the U.S., with whom the EU had maintained a dialogue on critical infrastructure protection since 2000. But even in this case, a working group more directly focused on cybersecurity and cybercrime was created in 2010, and most recently, in 2014, an EU-U.S. Cyber Dialogue was officially established to specifically address foreign policy issues related to cyberspace.

Nowadays, the EU also maintains cyber dialogues with Japan, South Korea and India and cyber is being integrated into enlargement and neighborhood relations, as is the case of the Western Balkans. For instance, the European Commission has recently adopted six flagship initiatives for the Western Balkans,[11] which include the development of cyber capabilities and the intensification of cooperation in order to address issues related to cybersecurity and cyber-crime. Also on a cyber-related front, the EU approved in June 2015[12] an Action Plan on Strategic Communication to specifically address Russia's "disinformation campaigns." A task force –East StratCom– was set up within the EEAS to report and analyze "disinformation narratives" and to work with eastern partners in terms of both developing "communication products and campaigns focused on better explaining EU policies" and to support "strengthening the media environment in the Eastern Partnership region."[13] The most visible outcome of this taskforce is its two weekly newsletters, the Disinformation Review and the Disinformation Digest that offer the latest trends in Russian trolling and regular fact-checking on Russian media.[14]

Consolidating Cyberspace in the European Union

In 2016, the EU Global Strategy placed cyber very much at the center of the EU's foreign policy,[15] in what was a sign of the progressive consolidations of cyberspace as a security and strategic priority within the EU. Among other aspects, the document presents the EU as a "forward-looking cyber player" that intends to protect its "critical assets and values in the digital world, notably by promoting a free and secure global Internet."[16] It wants to do so by "weaving cyber issues across all policy areas,"[17] in what can only be interpreted as an ambitious statement of intent.

Another cyber-related aspect mentioned in the strategy –hybrid threats– has also received close attention from Brussels. A joint framework from April 2016[18] set the main lines of action for the EU in this field in what was a clear response to Russia's activities in Ukraine. The document makes multiple references to cyber-related issues[19] and it defines five key actions regarding cybersecurity: (i) to intensify cooperation between member states and the EU in terms of emergency response teams; (ii) to further develop ties with the private sector in order to find solutions to protect critical infrastructures "against cyber aspects of hybrid threats"; (iii) to improve the security and resilience of electricity grids; (iv) to improve information-sharing with the financial sector; (v) and to coordinate responses with the transport sector in terms of responses to cyber-attacks. It also mentions the increase of cooperation with third countries in cyber-resilience and cyber-capacity building through the Instrument contributing to Stability and Peace[20] and it set out the details for the creation of a Hybrid Fusion Cell to be established in Finland –a symbolic gesture towards Russia. Hybrid warfare would also be at the center of the EU-NATO declaration

at the margins of the Warsaw NATO Summit in July 2016. The declaration sets a number of areas for cooperation, including building resilience in cyberspace[21] and developing shared capabilities in the field.

If 2013 was a crucial year for the EU in terms of its approach to cybersecurity, 2017 offered a more in-depth approach towards the issue. In June, the Council called for the development of a cyber diplomacy toolbox –eventually approved in October[22]– that will help the EU have a more coordinated and coherent international approach to cyberspace. The document is expected to lay out concrete measures to address malicious cyber-attacks, such as "the summoning of diplomats, further political, economic and penal sanctions, as well as digital responses."[23]A few months later, in September, Jean-Claude Juncker, in his State of the Union address, placed the security of Europe's critical information infrastructures at the center of its future.[24] That came a week after the Council approved a comprehensive cybersecurity package that, among other elements, proposes the creation of a new European Cybersecurity Research and Competence Centre and the development of an EU-based cybersecurity certification process.[25] Finally, 2017 was also the year the EU decided to set its Permanent Structured Cooperation (PESCO), in which two of its 17 projects will be explicitly dedicated to cyber defense.[26]

The current Commission team seems very much interested in developing the EU's cyber-capabilities, policies and infrastructures. Also, particular member states, such as Estonia seem to actively promote this agenda: both the cybersecurity package and the cyber diplomacy toolbox were elaborated and approved during this country's presidency of the EU in the second semester of 2017. Interviews recently conducted in Brussels with EU officials and representative of member states confirm the high level of activism in this field evidenced by the EU, with new measures, meetings and discussions on cyber-related topics now happening almost on a daily basis.

The development of so many new initiatives, and institutions, could potentially lead to a further fragmentation of the EU's approach to cybersecurity, with inter-institutional turf wars taking precedent over coherence and efficiency

One important aspect that remains to be seen is whether this activism will provide additional coherence to the EU's activities in the field. As we had the opportunity to argue elsewhere,[27] the initial stages of the EU's approach to cybersecurity have revealed a mismatch between what it wants to achieve in cyberspace and the means to do so. The increase in investment from the European Commission in the field may contribute to partially

From an EU perspective, when it comes to cyberspace, Russia should be seen as being, simultaneously, a cyber-crime hub, a neighbor, and an emerging power

address this issue, but much more needs to be done to have member states entirely aligned with the EU on this. As a policy area, they still are the main players when it comes to the European Union. Finally, the development of so many new initiatives, and institutions, could potentially lead to a further fragmentation of the EU's approach to cybersecurity, with inter-institutional turf wars taking precedent over coherence and efficiency.[28]

Russia, Cyber and Beyond

From what was presented so far it is already noticeable how Russia has been playing a central role in the EU's developments in the cyber field: it was after the 2007 Estonia attacks that cyber was seen as a relevant security dimension. Included in the 2008 Implementation Report, the 2015-2016 measures on hybrid warfare come as a follow up of Russia's invasion of Crimea and, more recently, Russia's interference in the U.S. and French elections –and potentially in the Brexit referendum– accelerated the Commission's interest in the field. In a recent report on EU-Russia relations[29] by the European Council on Foreign Relations, there were a total of 13 member states that feared Russia's interference in their domestic politics through hacking.[30]As clearly pointed out in a *Financial Times* article last year, "Russia is at the center of concern in Brussels about cybersecurity."[31]

If Russia's indirect influence in EU's cyber-activities is clearly visible, the EU's direct response to Moscow's activities is less so. The recently approved declaration on malicious cyber activity is a case in point. The Council Conclusions approved last April condemned "the malicious use of information and communications technologies (ICTs), including in WannaCry and NotPetya, which have caused significant damage and economic loss in the EU and beyond."[32] However, these declarations came over one year after the first of the two attacks –WannaCry– took place, and in neither case does it clearly attribute the responsibility for these attacks. Apparently, member states were very much divided regarding whether to do so, particularly given the sparse evidence available. This, despite the accusation by individual member states –the UK, Denmark, Lithuania and Estonia, with support from Latvia, Sweden and Finland[33]– that Russia was behind NotPetya. This case reflects two problems that are common to the EU's approach to cybersecurity. First, member states do not trust each other –or the EU, for that matter– sufficiently to share sensitive information that can lead to the attribution of cyber-attacks. Second, there is a delicate balance to have –specifically

On March 2018, the administrative computers of the German government were infiltrated with malware and the main suspect was the Russian hacker group APT28, also known as Fancy Bear.

Getty Images

for smaller member states– between accepting a more aggressive stance towards Moscow and the economic and geopolitical constraints when dealing with Russia. For some member states, Russia is an important economic partner and the biggest regional neighbor. This delicate balancing act that has often led to accusations of inconsistency and "strategic ambivalence,"[34] in terms of how the EU deals with Russia, is also present in cyberspace.

A Cyber-Balancing Act

Cyber is a broad policy field, cutting across multiple areas, from organized crime to the protection of water and energy supply infrastructures. In the same vein, it is important to recognize Russia as a multifaceted actor with whom to engage differently depending on the issue at hand. Most importantly, the EU does not engage with Russia on cyberspace only; most activities in this field are related to other policy areas and they need to be framed with that broader strategic engagement in mind. For Russia, cybersecurity is not even a valid starting point. Russia's doctrine is focused on information security, which translates to cyberspace the same logic that underpins the Soviet doctrine of information warfare in which the core principles are "that the psychological element of conflict [was] as important as the physical one."[35]According to the Information Security Doctrine adopted in September 2000: information security is "the protection of its [Russia's] national interests in the information sphere defined by the totality of balanced interests of the individual, society, and the state."[36] This rather comprehensive definition was updated in 2016, in which the infor-

mation sphere is defined as comprising the "combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet…, communication networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere."[37]

Following the *2017 Strategic Survey* from the London-based Institute of International and Strategic Studies, this all-encompassing, state-centric[38] definition of information security poses significant challenges to states that "considered themselves to be well prepared for purely technical cyber aggression, but had no defenses against a broader information offensive of which cyber-attacks were only one component,"[39] as was the case of the Russian involvement in the 2016 U.S. Presidential election.

Engaging with Russia

From an EU perspective, when it comes to cyberspace, Russia should be seen as being, simultaneously, a cyber-crime hub, a neighbor, and an emerging power. These are not mutually exclusive areas, but they certainly entail a set of different approaches in terms of how to engage with Russia. Starting with cyber-crime, it is well-known that Russia is a hub for cyber-criminal activity. In 2014, the company Group-IB calculated that the cyber-crime market in Russia to be valued at around $2.3 billion.[40] It is, however, important to distinguish between those attacks that are state-led or state-sponsored and those that are simply for-profit attacks. Russia's track record in this field is very concerning at both levels. However, whereas the first set of activities is intimately linked to broader strategic goals,[41] the second is not. In the same way the U.S. has agreed with China to cooperate on cyber-crime in 2015 –which at the time was seen as a victory for cyber diplomacy[42]– a similar arrangement could arguably be established between the EU and Moscow. And there are some precedents. Russia has cooperated with the EU on issues related to the use of the internet by terrorist organizations and even with Europol within the field of cyber-crime. But, overall, as concluded by Thomas Renard, "cooperation remains very limited."[43]

The Big Neighbor

For all the recent tensions, sanctions and aggressive stances, Russia remains the EU's biggest neighbor. One with whom European countries have significant economic interests, and even shared geopolitical concerns –Syria being a good example of the latter. This has two implications. Fist, when adopting an aggressive stance towards Moscow, the EU has to gauge the short and long-term consequences of those measures. Second, acknowledging Russia's neighboring status also means factoring in its potential impact on the EU's own neighborhood. According to Michael H. Smith and Richard Youngs that is already the case: the 'Russia factor' is now built into the EU's relations

with its Eastern neighbors to an extent that had not happened before.[44] When it comes to cyberspace, this means developing capabilities within the context of the European Partnership and the wider policy towards the Balkans, which, as we saw before, the EU is already doing.

Russia, the (Re)Emerging Power

Finally, Russia is also often dubbed as an emerging power. Although in the case of Russia that is certainly a misplaced label –it is neither 'emergent' nor necessarily a power on the same level as China or the U.S.– it has to be dealt with diplomatically within that context. That means engaging multilaterally, both cooperatively as was the case with the UN-sponsored Group of Governmental Experts on Information Security (GGE), but also by trying to limit Russia's international support for its own vision of cyberspace. In 2011, Vladimir Putin stated that Russia intended to use the International Telecommunication Union to monitor and control the internet,[45] a view that is very much in opposition to that of the EU. Also in 2011, China and Russia proposed the International Code of Conduct for Information Security through the Shanghai Cooperation Organization (SCO). That document gathered significant support amongst the developing nations that see the appeal in a sovereign-based international cyberspace system. However, this document has been severely criticized by the EU "over its insufficient guarantees for the lack of both the protection of human rights online and the multi-stakeholder model of the cyber domain."[46]

For all the recent tensions, sanctions and aggressive stances, Russia remains the EU's biggest neighbor. One with whom European countries have significant economic interests, and even shared geopolitical concerns

In addition, the EU and Russia frequently sit on opposing sides of the aisle when it comes to cyber-governance, as they often disagree on the basic terms of the discussion. The idea of sovereignty is a good example. For Russia, sovereignty is about a "top-down government from a single center, insulated from outside influence as well as from below," which differs from a more liberal and open understanding of sovereignty, that is very much at the basis of the European integration project. This, when in conjunction with Russia's great power ambitions and its willingness "to shape global norms, exercise veto rights, and dictate terms to others" only exacerbates the differences towards the rest of Europe.[47]

Conclusion

Dealing with Russia is always a balancing act, and cyberspace is not an exception. In the last few years the EU has been developing the tools to more forcefully and consistently engage in

The interior ministers from Germany, France, Italy, Poland, Spain and the UK meet in Germany for discussions focusing, among others, on the cyber-crime.

JENS SCHLUETER / AFP / Getty Images

the international realm of cyberspace. The cyber diplomacy 'toolbox' certainly is a step in the right direction, as is the cybersecurity 'package.'

It is however important to acknowledge that cyber-relations with Russia take place in a broader, complex context, both within and outside cyberspace. Within cyberspace, Russia is part –and often a leader– of a group of countries that views that fundamental formal and informal norms of cyberspace tilted towards the West, and in need of further 'democratization' and 'multilateralization.'[48] In this case, it is not about simply engaging with Russia, but with a set of significant stakeholders, both state and non-state actors, and to negotiate and assert the EU's positions when it comes to cyberspace. That is why cyber diplomacy should be seen as a central emerging practice for the EU. Outside of cyberspace, Russia understands its actions against member states and European institutions as part of a broader policy of destabilization and division in Europe. Russia operates in the information sphere, whereas the European Union tends to separate cyberspace from information operations. There are some clear signs that further articulation between these two aspects is being undertaken both at the European and national levels. The East StratCom is a good example of this, but more is certainly needed.

Russia's actions are often little more than "an improvised collection of activities engaged in by various actors who are linked together by an ideology that labels the West as an adversary."[49] Normalizing Russia, rather than treating it as a geopolitical powerhouse, would certainly contribute to improve relations with Moscow. It would also make it easier to understand that Russia can be a threat, but also a partner. In a recent article on the EU's stance within the context of a changing global

order, Michael H. Smith and Richard Youngs argue that the EU and many of its member states are adopting a *bounded containment* position regarding Russia. This is a position that "mixes elements that unwind interdependence with those that actually solidify the logic of inclusion in terms of talking with Russia on Ukraine's trade arrangements, internal political arrangements and conflict mediation issues."[50] This bounded containment needs to find a concrete translation to cyberspace, which involves the combination of deterrence and selective engagement measures with Russia. Fundamentally, it is important to acknowledge that responses will vary according to whether the interlocutor is Russia the neighbor, the emerging power or simply the cyber-crime hub. In all these dimensions there will be opportunities for cooperation, but also for conflict. The EU needs to be ready for both.

One of the ambitions of the 2016 EU Global Strategy is to promote the EU's "strategic autonomy."[51] When it comes to cyberspace, and in particular to Russia, that can only be achieved if the EU is pro-active[52] and most fundamentally if it is coherent.[53] For that to happen, member states will have to engage in more thorough trust-building exercises, both between themselves and with the EU institutions. They will have to accept the possibility of EU-wide responses to cyber-attacks, which may involve some limited offensive capability, and most fundamentally, the use of common resources to do so. The EU will need to have concrete tools to deter, respond and interact with Russia on cyberspace. It is challenging, but also inevitable.

When it comes to cyberspace, and in particular to Russia, that can only be achieved if the EU is pro-active and most fundamentally if it is coherent

Endnotes

1. For a historical overview of the EU's policy in this field see, George Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*, (London: Palgrave, 2016).

2. Such as the Council Framework Decision 2005/222/JHA on Attacks against Information Systems, the Regulation of the European Parliament and of the Council No 460/2004 establishing the European Network and Information Security Agency (ENISA), and the Communication from the Commission Towards a General Policy on the Fight against Cyber Crime.

3. As mentioned by Lucas Kello, "[b]efore the events in Estonia, no country had published a dedicated cybersecurity strategy; today dozens of countries have done so." Lucas Kello, *The Virtual Weapon and International Order*, (London: Yale University Press, 2018), p. 213.

4. Kello, *The Virtual Weapon*, p. 221.

5. See, Eneken Tikk, Kadri Kaska, *et al.*, "Cyber Attacks Against Georgia: Legal Lessons Identified," *NATO Cooperative Cyber Defence Centre of Excellence*, (November, 2008).

6. Where one can read: "attacks against private or government IT systems in EU Member States have given this a new dimension, as a potential new economic, political and military weapon." See, "Report on the Implementation of the European Security Strategy," *Council of the European Union*, (2008), p. 5.

7. Cybersecurity can be understood as "the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with

or that may harm its interdependent networks and information infrastructure. Cybersecurity strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein." See, "2013 EU Cybersecurity Strategy," *European Commission*, (2013), p. 3.

8. Directive 2013/40/EU of the European Parliament and of the Council of August 12, 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA.

9. The NIS sets some responsibilities and guidelines regarding the protection of critical information infrastructures in Europe, for both states and private companies. For a brief overview see, Charlie Maynard, Niek Ijzinga and Dick van Veldhuizen, "Why Do You Need to Know about the NIS Directive?" *Delloite*, retrieved from https://www2.deloitte.com/nl/nl/pages/risk/articles/why-do-you-need-to-know-about-the-nis-directive.html.

10. "Council Conclusions on Cyber Diplomacy," *Council of the European Union*, (February 11, 2015).

11. "Communication from the Commission to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions," *European Commission*, (2018), retrieved from https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf.

12. "European Council Meeting (March 19-20, 2015) – Conclusions," *General Secretariat of the Council,* (2015).

13. "Questions and Answers about the East StratCom Task Force," *EEAS*, (2017), retrieved from https://eeas.europa.eu/headquarters/headquarters-Homepage/2116/questions-and-answers-about-east-stratcom-task-force_en.

14. Thomas Holt, "Busting Russia's Fake News the European Union Way," *The Conversation*, (March 29, 2018), retrieved from https://theconversation.com/busting-russias-fake-news-the-european-union-way-93712.

15. For what it's worth, the prefix cyber appears 22 times in the document, a clear improvement from the number of times it appears on the 2003 European Security Strategy: 0.

16. "Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy," *EEAS*, (June, 2016), retrieved eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf p. 42.

17. "EU Global Strategy," p. 22.

18. Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats: a European Response," *European Commission*, (2016), retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=EN.

19. The prefix cyber appears 39 times in the document.

20. The IcSP is an EU instrument to support security initiatives and peace-building activities in partner countries. For more see, "Regulation (EU) No 230/2014 of the European Parliament and of the Council of 11 March 2014 Establishing an Instrument Contributing to Stability and Peace," *Official Journal of the European Union*, (2014), retrieved from http://ec.europa.eu/dgs/fpi/documents/140311_icsp_reg_230_2014_en.pdf.

21. "Joint Declaration by the President of the European Council, Donald Tusk, the President of the European Commission, Jean-Claude Juncker, and the Secretary General of NATO, Jens Stoltenberg," *European Union Council*, (July 8, 2016), retrieved from http://www.consilium.europa.eu/media/24293/signed-copy-nato-eu-declaration-8-july-en.pdf.

22. The document remains confidential for the time being.

23. Annegret Bendiek, Raphael Bossong and Matthias Schulze, "The EU's Revised Cybersecurity Strategy," *SWP*, (November, 2017), retrieved from https://www.swp-berlin.org/en/publication/revised-cybersecurity-strategy/.

24. "Press Release, State of the Union 2017 –Cybersecurity: Commission Scales up EU's Response to Cyber-attacks," *European Commission*, (September 19, 2017), retrieved from http://europa.eu/rapid/press-release.en.htm.

25. "Joint Communication to the European Parliament and the Council, Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU," *European Commission*, (September 19, 2017), retrieved from https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe.

26. Annegret Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," *SWP,* (April, 2018), retrieved from https://www.swp-berlin.org/en/publication/the-eu-as-a-force-for-peace-in-international-cyber-diplomacy/, p. 4.

27. Helena Carrapico and Andre Barrinha, "The EU as Coherent (Cyber) Security Actor?" *Journal of*

Common Market Studies, No. 55, Vol. 6 (2017), pp. 1254-1272.

28. Andre Barrinha and Helena Farrand-Carrapico, "How Coherent Is the EU Cybersecurity Policy?" *LSE EuroppBlog*, (2018), retrieved from http://blogs.lse.ac.uk/europpblog/2018/01/16/how-coherent-is-eu-cybersecurity-policy/.

29. Kadri Liik, "Winning the Normative War with Russia: An EU-Russia Power Audit," *European Council on Foreign Relations*, (2018), retrieved from http://www.ecfr.eu/publications/summary/winning_the_normative_war_with_russia_an_eu_russia_power_audit.

30. According to ECFR, these countries are: Austria, Bulgaria, Czech Republic, Denmark, Estonia, Germany, Hungary, Latvia, Lithuania, The Netherlands, Poland, Sweden and the United Kingdom.

31. Arthur Beesley, "EU Suffers Jump in Aggressive Cyber Attacks," *Financial Times*, (January 8, 2017), retrieved from https://www.ft.com/content/3a0f0640-d585-11e6-944b-e7eb37a6aa8e.

32. "Council Conclusions on Malicious Cyber Activities - Approval," *General Secretariat of the Council*, (April, 16, 2018), retrieved from p. 2.

33. Stilgherrian, "Blaming Russia for NotPetya Was Coordinated Diplomatic Action," *ZDNet*, (April 12, 2018), retrieved from https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action/.

34. Bendiek, "The EU as a Force for Peace in International Cyber Diplomacy," p. 7.

35. Kello, *The Virtual Weapon*, p. 227.

36. Cited in Hannes Ebert and Tim Maurer "Contested Cyberspace and Rising Powers," *Third World Quarterly*, Vol. 34, No. 6 (2013), p. 1066.

37. "Doctrine of Information Security of the Russian Federation," *Ministry of Foreign Affairs of the Russian Federation,* (December 5, 2016).

38. One of the main reasons why Russia has never signed the most important piece of international legislation in the field –the Budapest Convention is because it does not agree with Article 32 (b), that "allows owners of data to control its use, rather than governments," Russia "wants state control of information," David Ignatius, "Russia Is Pushing to Control Cyberspace: We Should All be Worried," *The Washington Post*, (October 24, 2017), retrieved from https://www.washingtonpost.com/opinions/global-opinions/russia-is-pushing-to-control-cyberspace-we-should-all-be-worried/2017/10/24/7014bcc6-b8f1-11e7-be94-fabb0f1e9ffb_story.html?noredirect=on.

39. "Strategic Survey: The Annual Assessment of Geopolitics," *IISS*, (September 20, 2017), p. 64.

40. Tim Maurer, "Why the Russian Government Turns a Blind Eye to Cybercriminals," *Slate*, (February 2, 2018), retrieved from https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html.

41. For instance, despite the frequent attribution of the 2007 Estonia attacks to Russia, the whole concrete evidence ever made public, solely links to Russian patriot hackers with no direct connection to the Russia state. For more see, P. W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, (Oxford: Oxford University Press, 2014).

42. André Barrinha and Thomas Renard, "Cyber-diplomacy: The Making of an International Society in the Digital Age," *Global Affairs*, (January 8, 2017), DOI: 10.1080/23340460.2017.1414924.

43. Thomas Renard, "EU Cyber Partnerships: Assessing the EU Strategic Partnerships with Third Countries in the Cyber Domain," *European Politics and Society*, Vol. 19, No. 3 (2018), p. 329.

44. Michael H. Smith and Richard Youngs, "The EU and the Global Order: Contingent Liberalism," *The International Spectator*, Vol. 53, No. 1 (2018), p. 51.

45. Ebert and Maurer, "Contested Cyberspace and Rising Powers," p. 1063.

46. Patryk Pawlak, "Cyber Security Woes: WannaCry?" *EUISS*, (May 13, 2017), p. 2.

47. Liik, *Winning the Normative War with Russia*, p. 3.

48. Chris C. Demchak , "Uncivil and Post-Western Cyber Westphalia: Changing Interstate Power Relations of the Cybered Age," *The Cyber Defense Review*, (Spring, 2016), pp. 49-74.

49. Liik, *Winning the Normative War with Russia*, p. 6.

50. Smith and Youngs, "The EU and the Global Order," p. 51.

51. "EU Global Strategy," p. 4.

52. As argued by Jakob Bund and Patryk Pawlak, "The EU's position as a norm-maker in other policy areas – notably on privacy and data protection – demonstrates its potential when it is more proactively involved." See, Jakob Bund and Patryk Pawlak, "Minilateralism and Norms in Cyberspace," *EUISS*, (September 25, 2017), retrieved from https://www.iss.europa.eu/content/minilateralism-and-norms-cyberspace, p. 2.

53. Carrapico and Barrinha, "The EU as Coherent (Cyber) Security Actor?"

LOCAL VIEWS ON GLOBAL NEWS.

READ DAILY TO KEEP UP WITH CHANGING TURKEY AND THE WORLD.

www.dailysabah.com

TURKUVAZ
MEDIA GROUP