The EUGS and Russian hybrid warfare: effective implementation but insufficient results

Maria Giulia Amadio Viceré
Post Doctoral Fellow in Political Science, LUISS University

Abstract

The 2016 EU Global Strategy (EUGS) defined the management of EU–Russia relations as a key strategic challenge for European security, and listed hybrid threats as among the most relevant dangers for Europe. In the framework of the Strategy's implementation, the EU sought to counter the Kremlin's cyberwarfare and its disinformation campaigns through a series of valuable initiatives across different policy sectors. While doing so, the Union has generally ensured the coherence between its external and internal policies and increased its cooperation with NATO. Although most of the EUGS's provisions on cybersecurity and strategic communication have been implemented, additional efforts would be needed to effectively counter Russian hybrid warfare. On the one hand, the EU approach on these matters is still marred by institutional and financial fragmentation within the EU and between Brussels and EU Member States. On the other, the EU still devotes relatively limited resources to countering Russian disinformation and cyber attacks, especially if compared to the Kremlin's investments.

March 2019

Following the annexation of Crimea and the ensuing worsening of EU–Russia relations, Moscow's strategy in cyberspace has been increasingly hostile and assertive. While Europe's multiple crises have been impacting on citizens' everyday lives, Russia has been making full use of its influence on traditional and social media to inject confusion and ignite fears in EU politics. Against this backdrop, the 2016 EU Global Strategy (EUGS) defined the management of the EU's relationship with Russia as a key strategic challenge for the European security order, and listed hybrid threats among the most relevant dangers for Europe.[1] In this context, the Strategy put particular emphasis on the need to increase the EU's focus on cybersecurity and to enhance its strategic communication.

Cybersecurity

In the post EUGS era, Brussels has devoted particular attention to cybersecurity issues. In September 2017 the Union revised its cybersecurity strategy with the aim of increasing EU resilience in this sector,[2] and in June 2017 the European Council drafted a cyber diplomacy toolbox.[3] New forms of political, operational and technical cooperation among national governments were also established. In the framework of the Permanent Structured Cooperation (PESCO), Member States launched a project on cyber response and mutual assistance, which intends to bring together their expertise through the creation of EU Cyber Rapid Response Force Teams (CRRTs).[4]

Meanwhile, the Union has developed integrated cybersecurity assessments amongst EU and national institutions. Shortly after becoming operational within the European External Action Service in July 2017, the Hybrid Fusion Cell began to meet regularly with Member States' focal points. Notably, in 2018 cyber analytical components were also added to the Cell to increase EU situational awareness after the Salisbury attacks.[5] Moreover, a project initiated under PESCO is currently creating a Cyber Threats and Incident Response Information Sharing Platform.[6]

As explicitly envisaged in the EUGS, cybersecurity issues were embedded in different public policy sectors. The EU institutions' Computer Emergency Response Team intensified cooperation with Member States on cybersecurity threats in critical areas such as transport, communications, space

[1] European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, Brussels, 24 June 2016, https://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web_0.pdf
[2] European Commission, *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU,* Brussels, 13 September 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN
[3] European Council, *Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions,* Brussels, 19 June 2017, https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
[4] European External Action Service, *New Tool to Address Cyber Threats: The EU's Rapid Response Force,* 27 June 2018, https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en
[5] European Commission, *A Europe That Protects: EU Works to Build Resilience and Better Counter Hybrid Threats*, Brussels, 13 June 2018, http://europa.eu/rapid/press-release_IP-18-4123_en.htm
[6] EU, *Cyber Threats and Incident Response Information Sharing Platform,* 2018, https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/

FEPS | Rue Montoyer 40, B-1000 Brussels | Tel + 32 2 234 69 00 | Fax + 32 2 280 03 83 | info@feps-europe.eu

and finance.[7] In addition to this, while the Commission continued supporting the European Energy Information Sharing and Analysis Centre on cybersecurity,[8] in June 2018 it also began to actively assist Member States in implementing the Directive on Security of Network and Information Systems (NIS Directive) in this policy area.[9] The Strategy's provision on the establishment of public–private partnership was implemented as well. Thus, in July 2016 the European Commission signed a contractual arrangement on industrial research and innovation with the European Cyber Security Organization Association.[10]

In line with the EUGS's commitments, Brussels has enhanced its cooperation with the Atlantic Alliance in cybersecurity. Since 2017 the EU and NATO have each held a seat on the Steering Board of the European Centre of Excellence for Countering Hybrid Threats, which supports the development of best practices and efforts through research and training activities including in the cyber domain.[11] In this context, the EU Hybrid Fusion Cell has been coordinating daily with NATO's Hybrid Analysis Branch.[12] Furthermore, a series of EU–NATO exercises aimed at improving cooperation on cybersecurity took place in the past years under the 2016 EU Playbook.[13]

Although the majority of the EUGS provisions on cybersecurity have been implemented, several cyber espionage and hacking activities linked to Russia have successfully targeted EU institutions and Member States in recent years.[14] In fact, persistent institutional and financial fragmentation within the EU and between Brussels and the Member States, coupled with insufficient resources, has overshadowed the EU's ability to counter cyber attacks.[15]

[7] European Commission, *Joint Report on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018,* Brussels, 13 June 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/46398/joint-report-implementation-joint-framework-countering-hybrid-threats-july-2017-june-2018_en

[8] European Commission, *Cybersecurity Package "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"*, Brussels, 19 September 2017, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

[9] European Commission, *The Directive on Security of Network and Information Systems (NIS Directive),* Brussels, 24 August 2018, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

[10] European Commission, *Commission Decision to Establish a Contractual Public Private Partnership on Cybersecurity (cPPP)*, Brussels, 5 July 2016, https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp

[11] See: The European Centre of Excellence for Countering Hybrid Threats, *What Is Hybrid COE?*, 2019, https://www.hybridcoe.fi/what-is-hybridcoe/

[12] European Parliament, *Parliamentary Questions*, 12 January 2018, http://www.europarl.europa.eu/doceo/document/E-8-2017-005865-ASW_EN.html?redirect

[13] European Commission, *Security and Defence: Significant Progress to Enhance Europe's Resilience against Hybrid Threats – More Work Ahead*, Brussels, 19 July 2017, http://europa.eu/rapid/press-release_IP-17-2064_en.htm

[14] Jarno Limnell, "Russian Cyber Activities in the EU", in Nicu Popescu and Stanislav Secrieru (eds.), *Hacks, Leaks and Disruptions: Russian Cyber Strategies,* Paris, European Union Institute for Security Studies, 2018

[15] Camino Mortera-Martinez, "Game Over? Europe's Cyber Problem", in *Centre For European Reform*, July 2018, https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem

FEPS | Rue Montoyer 40, B-1000 Brussels | Tel + 32 2 234 69 00 | Fax + 32 2 280 03 83 | info@feps-europe.eu

Strategic Communication

Within the framework of the EUGS implementation, the Union has responded to Russian interference in European politics by increasing the uniformity and rapidity of its communication. The Stratcom Task Force has been confuting pro Kremlin campaigns on social media.[16] At the same time, it has been actively engaged in improving the Union's public diplomacy by publishing analytical articles, and by recommending reliable studies and reports on pro Russian disinformation.[17]

Indeed, EU external policies on strategic communication developed within the Strategy's implementation have been consistent with internal initiatives over time. From 2017 to 2018 the European Commission doubled its funds for projects run by the European Centre for Press and Media Freedom.[18] Moreover, in 2018 the European Parliament allocated 750,000 euros for adaptation of the Media Pluralism Monitor to the digital environment.[19] In the meantime, following the April 2018 Action Plan,[20] in October 2018 Facebook, Google, Twitter and Mozilla, as well as representatives of online platforms and the advertising industry, signed the EU Code of Practice against Disinformation.[21] In this context, in December 2018 the European Commission also requested online platforms to provide monthly reports on their controls over the integrity of the coming European electoral processes.[22]

Despite the implementation of all the EUGS's provisions on strategic communication, the EU's efforts against Russian disinformation have not delivered the desired results up until now. Moscow managed to spread fake news concerning the 2016 constitutional Italian referendum,[23] in the run up to the German federal voting,[24] and in the Catalan crisis.[25] Added to this, evidence suggests that Russian Twitter accounts have tried to influence the Italian 2018 general elections.[26] As a matter of fact, the EU has been devoting limited resources to the enhancement of its public diplomacy,

[16] EU vs. Disinformation Account on Facebook, https://www.facebook.com/EUvsDisinfo/; and The EU Mythbusters Account on Twitter, https://twitter.com/EUvsDisinfo
[17] EU vs. Disinfo, *Reading List*, 2018, https://euvsdisinfo.eu/reading-list/
[18] European Commission, *Media Freedom Projects,* Brussels, 28 November 2018, https://ec.europa.eu/digital-single-market/en/media-freedom-projects
[19] European Commission, *Monitoring Media Pluralism in the Digital Era,* Brussels, 18 January 2019, https://ec.europa.eu/digital-single-market/en/media-pluralism-monitor-mpm
[20] European Commission, *Tackling Online Disinformation: A European Approach,* Brussels, 26 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236
[21] European Commission, *Code of Practice on Disinformation,* Brussels, 26 September 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation
[22] European Commission, *Action Plan against Disinformation*, Brussels, 5 December 2018, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf
[23] Jacopo Iacobini, "The Russian Propaganda against Renzi: And Grillo's Web Backs It Up", in *La Stampa*, 11 November 2016, https://www.lastampa.it/2016/11/11/esteri/lastampa-in-english/the-russian-propaganda-against-renzi-and-grillos-web-backs-it-up-aJjrmPmt1Y17Xv5UbgmJaL/pagina.html
[24] Mark Scott, "Russian 'Botnet' Promotes Far-Right Messages in German Election", in *Politico*, 24 September 2017, https://www.politico.eu/article/russian-botnet-promotes-far-right-messages-in-german-election/
[25] Davide Alandete, "Russian Network Used Venezuelan Accounts to Deepen Catalan Crisis", in *El Pais*, 11 November 2017, https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html
[26] Paolo Mastrolilli, "How Russian Twitter Accounts Are Trying to Influence the Italian Vote", in *La Stampa*, 17 February 2018

FEPS | Rue Montoyer 40, B-1000 Brussels | Tel + 32 2 234 69 00 | Fax + 32 2 280 03 83 | info@feps-europe.eu

especially if compared to Moscow's investments for its disinformation activities. The EU East Stratcom Task Force is a case in point. While the Task Force currently has a budget of 1.1 million euros, the budget of RT – just one of the news outlets funded by the Kremlin – is estimated to be 300 million euros a year.[27]

Conclusion

Indeed, most of the EUGS's provisions on cybersecurity and strategic communication have been implemented. As reflected in the revision of the EU cybersecurity strategy and by the launch of two PESCO projects, the Union has introduced new forms of cooperation in the cyber domain. In doing so, Brussels has embedded cybersecurity issues in different public policy sectors and established public–private partnerships. Furthermore, EU–NATO cooperation against hybrid threats has increased through joint activities. In the meantime, the EU has strengthened its strategic communication through Stratcom Task Force activities, while supporting initiatives aimed at fostering pluralism within the EU media environment.

Nonetheless, as the continuation and extension of Russian hybrid warfare in recent years demonstrates, the Strategy's implementation has been less than effective. In fact, the EU approach on these matters is still marred by institutional and financial fragmentation. Added to this, Brussels devotes limited resources to countering Russian hybrid warfare, especially if compared to the Kremlin's investments. As the 2019 European elections are approaching, the EU should do its best to fill the gap between a reasonably complete implementation and an efficient one.

[27] Georgi Gotev, "Experts Lament Underfunding of EU Task Force Countering Russian Disinformation", in *EurActiv,* 23 November 2018, https://www.euractiv.com/section/global-europe/news/experts-lament-underfunding-of-eu-task-force-countering-russian-disinformation/

FEPS | Rue Montoyer 40, B-1000 Brussels | Tel + 32 2 234 69 00 | Fax + 32 2 280 03 83 | info@feps-europe.eu

References

Alandete, Davide, "Russian Network Used Venezuelan Accounts to Deepen Catalan Crisis", in *El Pais*, 11 November 2017, https://elpais.com/elpais/2017/11/11/inenglish/1510395422_468026.html

European Commission, *Commission Decision to Establish a Contractual Public Private Partnership on Cybersecurity (cPPP)*, Brussels, 5 July 2016, https://ec.europa.eu/digital-single-market/en/news/commission-decision-establish-contractual-public-private-partnership-cybersecurity-cppp

European Commission, *Security and Defence: Significant Progress to Enhance Europe's Resilience against Hybrid Threats – More Work Ahead*, Brussels, 19 July 2017, http://europa.eu/rapid/press-release_IP-17-2064_en.htm

European Commission, *Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU,* Brussels, 13 September 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1505294563214&uri=JOIN:2017:450:FIN

European Commission, *Cybersecurity Package "Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU"*, Brussels, 19 September 2017, https://ec.europa.eu/digital-single-market/en/news/cybersecurity-package-resilience-deterrence-and-defence-building-strong-cybersecurity-eu

European Commission, *Tackling Online Disinformation: A European Approach,* Brussels, 26 April 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

European Commission, *A Europe That Protects: EU Works to Build Resilience and Better Counter Hybrid Threats*, Brussels, 13 June 2018, http://europa.eu/rapid/press-release_IP-18-4123_en.htm

European Commission, *Joint Report on the Implementation of the Joint Framework on Countering Hybrid Threats from July 2017 to June 2018,* Brussels, 13 June 2018, https://eeas.europa.eu/headquarters/headquarters-homepage/46398/joint-report-implementation-joint-framework-countering-hybrid-threats-july-2017-june-2018_en

European Commission, *The Directive on Security of Network and Information Systems (NIS Directive),* Brussels, 24 August 2018, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Commission, *Code of Practice on Disinformation,* Brussels, 26 September 2018, https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

European Commission, *Media Freedom Projects,* Brussels, 28 November 2018, https://ec.europa.eu/digital-single-market/en/media-freedom-projects

FEPS | Rue Montoyer 40, B-1000 Brussels | Tel + 32 2 234 69 00 | Fax + 32 2 280 03 83 | info@feps-europe.eu

European Commission, *Action Plan against Disinformation*, Brussels, 5 December 2018, https://ec.europa.eu/commission/sites/beta-political/files/eu-communication-disinformation-euco-05122018_en.pdf

European Commission, *Monitoring Media Pluralism in the Digital Era,* Brussels, 18 January 2019, https://ec.europa.eu/digital-single-market/en/media-pluralism-monitor-mpm

European Council, *Cyber Attacks: EU Ready to Respond with a Range of Measures, Including Sanctions,* Brussels, 19 June 2017, https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

European External Action Service (EEAS), *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, Brussels, 24 June 2016, https://europa.eu/globalstrategy/sites/globalstrategy/files/regions/files/eugs_review_web_0.pdf

European External Action Service, *New Tool to Address Cyber Threats: The EU's Rapid Response Force,* 27 June 2018, https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en

European Parliament, *Parliamentary Questions*, 12 January 2018, http://www.europarl.europa.eu/doceo/document/E-8-2017-005865-ASW_EN.html?redirect

EU, *Cyber Threats and Incident Response Information Sharing Platform,* 2018, https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/
EU vs. Disinfo, *Reading List*, 2018, https://euvsdisinfo.eu/reading-list/

Gotev, Georgi, "Experts Lament Underfunding of EU Task Force Countering Russian Disinformation", in *EurActiv,* 23 November 2018, https://www.euractiv.com/section/global-europe/news/experts-lament-underfunding-of-eu-task-force-countering-russian-disinformation/

Iacobini, Jacopo, "The Russian Propaganda against Renzi: And Grillo's Web Backs It Up", in *La Stampa*, 11 November 2016, https://www.lastampa.it/2016/11/11/esteri/the-russian-propaganda-against-renzi-and-grillos-web-backs-it-up-aJjrmPmt1Y17Xv5UbgmJaL/pagina.html

Limnell, Jarno, "Russian Cyber Activities in the EU", in Nicu Popescu and Stanislav Secrieru (eds.), *Hacks, leaks and Disruptions: Russian Cyber Strategies,* Paris, European Union Institute for Security Studies, 2018

Mastrolilli, Paolo, "How Russian Twitter Accounts Are Trying to Influence the Italian vote", in *La Stampa*, 17 February 2018

Mortera-Martinez, Camino, “Game Over? Europe's Cyber Problem”, in *Centre for European Reform*, July 2018,
https://www.cer.eu/publications/archive/policy-brief/2018/game-over-europes-cyber-problem

Scott, Mark, “Russian ‘Botnet’ Promotes Far-Right Messages in German Election”, in *Politico*, 24 September 2017,
https://www.politico.eu/article/russian-botnet-promotes-far-right-messages-in-german-election/

The EU Mythbusters Account on Twitter, https://twitter.com/EUvsDisinfo

The European Centre of Excellence for Countering Hybrid Threats, *What Is Hybrid COE?* , 2019, https://www.hybridcoe.fi/what-is-hybridcoe/

FEPS | Rue Montoyer 40, B-1000 Brussels | Tel + 32 2 234 69 00 | Fax + 32 2 280 03 83 | info@feps-europe.eu