UIbrief
No.7
2017
PUBLISHED BY THE SWEDISH INSTITUTE
OF INTERNATIONAL AFFAIRS. WWW.UI.SE

Cybersecurity: the effects of Trump presidency and Brexit

Sarah Backman

The cybersecurity challenges facing Europe today and in the future are many and complex. The British exit from the EU (usually referred to as "Brexit"), in combination with the presidency of Donald Trump has forced European security cooperation into a phase of uncertainties and turbulence, whose outcome is still unknown. At the same time, Europe faces unprecedented digital threats.

The transboundary nature of cyber threats in combination with increasing societal dependence on cyberspace makes it hard to fully grasp their potentially disruptive impact. Cyber incidents affect individuals, businesses and nations alike, and the frequency of these incidents is increasing rapidly. Cybercrime "as a service" has become more and more common. EC3 (European Cybercrime Centre) stated in its annual threat report from 2016 that "the additional increase in volume, scope and financial damage combined with the asymmetric risk that characterizes cybercrime has reached such a level that in some EU countries cybercrime may have surpassed traditional crime in terms of reporting". At the same time, European critical infrastructure has proved vulnerable to cyberattacks that seek financial gain, with the WannaCry ransomware attacks on hospitals and organizations during May 2017 – the most extensive attack ever of its kind – setting a fearsome example. Moreover, in late 2016, security researchers uncovered "Operation Cloud Hopper" – a cyber espionage campaign conducted by a China-based threat actor, which targeted managed IT service providers (MSPs),

allowing the attackers unprecedented potential access to sensitive data and intellectual property. 2016 also marked a shift in the cyberattack landscape towards campaigns designed to influence political outcomes, such as disinformation campaigns. Generally, the use of offensive cyber power has become more and more likely a result of an increasing number of attacks for subversive purposes.

On the 8th of May 2017, the European Political Strategy Centre (European Commission) issued a Strategic Note called "Building an Effective European Cyber Shield – taking EU Cooperation to the Next Level." It clearly states that Europe is currently insufficiently prepared to successfully meet the requirements of cybersecurity in the present cyber threat and risk landscape. It emphasizes the importance and urgency of the European Union and its Member States to make cyber capability a political priority, quickly scale up European cybersecurity cooperation and individual Member State cybersecurity capabilities, and anticipate a plan "for hitherto unimaginable scenarios in which they would be put under severe [cyber] attack". A swift roll out of the recent NIS (Network and Information Security) - Directive, aiming to improve cyber capabilities and cooperation across the EU, will be important, says the strategic note – but the EU and Member States must already consider enhancing competence sharing beyond that. Europe faces great challenges in improving the currently uneven cyber capabilities across the continent, lacking information sharing and cooperation between various stakeholders, as well as a still lacking general awareness of cyber threats and their possible implications.

In this new and darker phase of digital development, horizontal collaboration (such as between states and between private and public actors), as well as vertical collaboration between, for example, the technical and strategic levels is key. Strengthening international collaboration and information sharing has long been considered one of the most important EU measures regarding cybersecurity, which has resulted in several new EU cybersecurity collaboration initiatives such as the CSIRT network – consisting of Member State CSIRTs (Computer Security Incident Response Teams) and CERT-EU (Computer Emergency Response Team of the EU institutions), the Cooperation Group (consisting of representatives of Member States, European Agency of Network and Information Security (ENISA) and the European Commission) and a new public private partnership on cybersecurity (with ECSO, European Cyber Security Organization).

Considering the grave situation regarding cyber threats and the dire need for improved European cybersecurity collaboration, how will Brexit affect European cybersecurity and the EU cybersecurity initiatives?

It is clear that the UK has strong incentives to continue promoting increasing cybersecurity capabilities, cooperation and information sharing within Europe, not least due to the cross-border nature of cyber threats and the likeliness of a domino-effect should a major cyber crisis hit the continent. Cybersecurity is indeed one of the areas specifically mentioned by the UK as an important area of continuous cooperation when leaving the EU.[1] Thus, it is likely that we will see the UK still supporting EU initiatives and objectives regarding

cybersecurity and cybersecurity collaboration. It is difficult at this point to foresee exactly how post-Brexit UK-EU cooperation on cybersecurity will look like. Naturally, the UK will lose some of its current influence regarding EU cybersecurity laws and policies. New agreements between the EU and the UK will also have to be negotiated. The new EU privacy-regulation GDPR (General Data Protection Regulation) which has to be implemented into Member State law by May 2018 will most likely continue be implemented in British law, which will ease cooperation and trade.

However, information sharing and capability sharing between the UK and the EU will probably decrease as a result of UK's diminished role in EU cybersecurity collaboration initiatives and institutions like the CSIRT-Network and the EC3 (European Cybercrime Centre). Moreover, interoperability might suffer as a result of less interaction between key cybersecurity personnel.

As a result of Brexit, the UK will likely promote European cybersecurity more through NATO, for example via CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence) and will work towards increasing EU-NATO collaboration on cybersecurity matters. Signs of the British move towards promoting cooperation between the two are already visible. In March 2017, Stephen Lovegrove, the British Defence Ministry's permanent secretary, called for greater NATO-EU cooperation on cybersecurity at the Atlantic Council. That same month Michel Fallen, British Defence Secretary urged the EU to "cooperate more closely with NATO, to avoid unnecessary duplication and to work together on new threats, including cyber." at a meeting of EU defence ministers in Brussels.[2] NATO, especially in case of weakened support from the US, might in return benefit greatly from the UK (being one of the most cybersecurity mature countries in Europe and, arguably, the world) stepping up its commitment to NATO cybersecurity issues and pushing NATO-EU cyber collaboration forward. The prospects for a closer collaboration had indeed been strengthened by Brexit, but likewise by new agreements on closer EU-NATO cybersecurity cooperation. For example, the NATO-EU joint declaration presented at the NATO Warsaw summit 2016, EU and NATO states its intentions to strengthen their relationship by introducing (for the first time in the EU-NATO relations) an official set of interlinked and complementary activities in cyber defence and cybersecurity.[3] Moreover, proposals for increased information sharing have been discussed at high level staff dialogues between EU and NATO. [4]

However, the question remains: to what extent will increased cyber information sharing within Europe be achieved? Cybersecurity information is often sensitive in nature, which creates a natural reluctance to share it. In order to enhance information sharing, trust has to be further developed. The preconditions for such trust to develop among European actors has certainly been severely weakened by Brexit and the Eurosceptic winds connected to it, regardless of closer EU-NATO cybersecurity cooperation and the UK's motivation to continue its cybersecurity cooperation with the EU. And without continuous development of trust, cybersecurity cooperation at the European level may stall, with the result that bilateral

or regional structures will instead be the settings of deep cybersecurity cooperation in Europe.

When it comes to the effects of the Trump presidency on European cybersecurity, the aspect of trust is central as well. Trump's protectionism and Jacksonian unilateral focus, as well as his favoring of "hard power" over "soft power", lead us to expect that he will promote the narrative of cybersecurity as a defence and individual national security issue. This is in contrast to the EU's narrative of cybersecurity as a shared challenge which requires extensive and rather deep international collaboration and information sharing.

President Trump has continuously discussed the importance of cybersecurity, calling it one of the US' most critical national security concerns. Showing his commitment to enhancing US cybersecurity, Trump issued an executive order the 11th of May 2017 called "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", which presents cybersecurity as a national security priority and tasks the DHS to assess and report on a number of key actions in order to, among other things, secure critical infrastructures. In line with our expectations on his focus on "hard power", Trump has continuously emphasized the need for the US to gain increased cyber counterattack capabilities, which would include greater retaliation against (especially state-sponsored) attacks.[5]

It remains to be seen exactly how the Trump administration will engage in international cybersecurity collaboration and develop cybersecurity policy. As part of the executive order issued in May, an international cybersecurity engagement strategy will be developed in addition to international cybersecurity priorities. This strategy will give more clarity in President Trump's ambitions and what we can expect in the next few years regarding US-Europe cybersecurity collaboration.

However, it is clear that President Trump takes cybersecurity seriously and will try to enhance the United States cybersecurity level generally. It is also clear that he aims to enhance the US offensive cyber capabilities and that he views cyber capability as a "hard power", with less emphasis on international collaboration. President Trump has also shown little interest in increasing or deepening security cooperation within NATO or with the EU, a stance which will probably include cybersecurity.

This may lead to a more cyber-resilient and cyber-secure United States, but it might also lead to a more hostile international cyber environment with increased tensions and risk for cyber conflict. It will definitely present a challenging international environment for Europe to develop trust, cybersecurity collaboration and common capabilities in.

Sarah Backman is a cyber security consultant at the Secana and research analyst at Stockholm University (SU)

[1] https://www.ft.com/content/2deb3c7c-0ca7-11e7-b030-768954394623

[2] http://www.atlanticcouncil.org/blogs/new-atlanticist/british-official-calls-for-greater-nato-eu-cybersecurity-cooperation

[3] http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/

[4] https://eeas.europa.eu/headquarters/headquarters-homepage_en/15917/NATO%20and%20EU%20press%20ahead%20with%20cooperation%20on%20cyber%20defence

[5] Little, Seifert, Gorman "Cybersecurity under the Trump Administration", Brunswick 2016

UIbrief

WOULD YOU LIKE TO KNOW MORE ABOUT UI?

The Swedish Institute of International Affairs (UI) is an independent platform for research and information on foreign affairs and international relations.

The institute's experts include researchers and analysts specialized in the field of international affairs. While maintaining a broad perspective, research at UI focuses on unbiased scientific analysis of foreign and security policy issues of special relevance to Sweden. UI as an organization does not take a stand on policy issues.

UI Briefs are short commentaries on international issues, events or trends related to UI's focus areas. They are written by UI staff, UI visiting researchers, or other experts associated with UI. UI Briefs do not require adherence to strict academic conventions. While the author is responsible for the text, the relevant programme director and one additional researcher have reviewed each manuscript.

For more information visit our website: www.ui.se, where you will find up-to-date information on activities at the Swedish Institute of International Affairs (UI). Here you can book seminar tickets, become a member, buy copies of our magazines, and access research publications. You can get in touch with us through email: **info@ui.se or +46-8-511 768 05**

Also, follow us on Twitter @UISweden or like us on Facebook!

SWEDISH INSTITUTE OF INTERNATIONAL AFFAIRS
Visiting Adress: Drottning Kristinas väg 37, Stockholm
Postal Adress: Box 27 035, 102 51 Stockholm
Phone: +46 8 511 768 05 Fax: + 46 8 511 768 99
Homepage: www.ui.se