Cybersecurity was back in the spotlight earlier in October, when several Western countries issued a coordinated denunciation of Russia, accusing it of running a global hacking campaign. Moscow denied the allegations. On 4 October, the UK and the Netherlands accused Moscow of sending agents to The Hague to hack into the Organisation for the Prohibition of Chemical Weapons, while the United States indicted suspected Russian agents for conspiring to hack computers and steal data to delegitimise international anti-doping organisations. They were also accused of trying to hack into Westinghouse Electric, a nuclear power company.

Russia and other countries had earlier been accused of cyber-espionage, proliferation of fake news, and misuse of social media in some election campaigns. Cybersecurity can be defined as the protection of computer systems and mobile devices from theft and damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide.

This note offers links to reports and commentaries from major international think-tanks and research institutes on cyber-security and related issues. More reports on the topic can be found in a previous edition of 'What Think Tanks are thinking', published in April 2018.

Hacks, leaks and disruptions: Russian cyber strategies
European Union Institute for Security Studies, October 2018

Intelligence artificielle: Vers une nouvelle révolution militaire?
Institut français des relations internationales, October 2018

The future of financial stability and cyber risk
Brookings Institution, October 2018

Disinformation on steroids
Council on Foreign Relations, October 2018

Olympic-caliber cybersecurity: Lessons for safeguarding the 2020 Games and other major events
Rand Corporation, October 2018

Sharing is caring: The United States’ new cyber commitment for NATO
Council on Foreign Relations, October 2018

Extending federal cybersecurity to the endpoint
Center for Strategic and International Studies, October 2018

Shifting borders and new technological frontiers: The case of Italy
Istituto Affari Internazionali, September 2018
Is China still stealing Western intellectual property?
Council on Foreign Relations, September 2018

Defining Russian election interference: An analysis of select 2014 to 2018 cyber enabled incidents
Atlantic Council, September 2018

Facebook, Twitter, and the challenge from Washington
Council on Foreign Relations, September 2018

Who’s afraid of a digital planet?
Brookings Institution, September 2018

Tech companies must do more to secure U.S. elections from authoritarian interference
German Marshall Fund, September 2018

Cognitive effect and state conflict in cyberspace
Center for Strategic and International Studies, September 2018

Sécurité numérique des objets connectés, l’heure des choix
Fondation pour la Recherche Stratégique, September 2018

How Ukraine’s government has struggled to adapt to Russia’s digital onslaught
Council on Foreign Relations, August 2018

China’s Junmin Ronghe and cybersecurity
Istituto per gli Studi di Politica Internazionale, August 2018

Developing cybersecurity capacity: A proof-of-concept implementation guide
Rand Corporation, August 2018

Eliminating a blind spot: The effect of cyber conflict on civil society
Council on Foreign Relations, August 2018

The disconnected dots between meddling and collusion
Cato Institute, August 2018

How Chinese cybersecurity standards impact doing business in China
Center for Strategic and International Studies, August 2018

Game over? Europe’s cyber problem
Centre for European Reform, Open Society European Policy Institute, July 2018

Cybercrime as a threat to international security
Istituto per gli Studi Politiica Internazionale, July 2018

No middle ground: Moving on from the crypto wars
European Council on Foreign Relations, July 2018

Using social media and social network analysis in law enforcement
Rand Corporation, July 2018

Cybersécurité: Une question de confiance
Confrontations Europe, July 2018
Protecting Europe against software vulnerabilities: It’s time to act!
Centre for European Policy Studies, June 2018

Géopolitique de la cyber-conflictualité
Institut français des relations internationales, June 2018

Shaping responsible state behavior in cyberspace
German Marshall Fund, June 2018

Software vulnerability disclosure in Europe: Technology, policies and legal challenges
Centre for European Policy Studies, June 2018

Cybersecurity in finance: Getting the policy mix right
Centre for European Policy Studies, June 2018

A balance of power in cyberspace
The Hague Centre for Strategic Studies, 2018

E-emblems: Protective emblems and the legal challenges of cyber warfare
Istituto Affari Internazionali, June 2018

Russian election interference: Europe’s counter to fake news and cyber attacks
Carnegie Europe, May 2018

Cybersecurity in an age of insecurity
Observer Research Foundation, May 2018

Attribution in cyberspace: Beyond the “Whodunnit”
GLOBSEC Policy Institute, May 2018

Speed and security: Promises, perils, and paradoxes of accelerating everything
Rand Corporation, May 2018

DISCLAIMER AND COPYRIGHT
This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.
Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.
eprs@ep.europa.eu (contact)
www.eprs.ep.parl.union.eu (intranet)
www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)