Briefing
What Think Tanks are thinking
27 April 2018

Cyber-security

Cyber-security 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. Cyber-crime and cyber-attacks have become a growing threat to governments, businesses and individuals as digital technologies advance. There have also been allegations of cyber-espionage, proliferation of fake news and misuse of social media in some electoral campaigns. The European Commission updated the European Union's cyber-security strategy in September 2017, to promote cyber-resilience and joint response across the bloc.

This note offers links **to reports and commentaries from some major international think-tanks and research institutes** on cyber-security and relations issues. More reports on the topic can be found in a previous edition of 'What Think Tanks are thinking', published in February 2017.

The 'known unknowns' of Russian cyber signalling
Council on Foreign Relations, April 2018

Fighting fake news: Caught between a rock and a hard place
European Council on Foreign Relations, March 2018

Europe's cyber problem
Centre for European Reform, March 2018

Non-proliferation regime for cyber weapons: A tentative study
Istituto Affari Internazionali, March 2018

The future of political warfare: Russia, the West, and the coming age of global digital competition
Brookings Institution, March 2018

Significant cyber incidents
Center for Strategic and International Studies, March 2018

The next Russian attack will be far worse than bots and trolls
Brookings Institution, March 2018

Offensive cyberattacks would need to balance lawful deterrence and the risks of escalation
Chatham House, March 2018

The West's confusion over Russia's cyberwars
Carnegie Europe, March 2018

EU cybersecurity and the paradox of progress
Centre for European Policy Studies, February 2018

Cybersécurité des infrastructures énergétiques: Regards croisés Europe/États-Unis
Institut français des relations internationales, February 2018

EPRS | European Parliamentary Research Service
Author: Marcin Grajewski, Strategy and Coordination Unit

EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain
Egmont, February 2018

Economic impact of cybercrime: No slowing down
Center for Strategic and International Studies, February 2018

Hacking for influence: Foreign influence activities and cyber-attacks
International Centre for Defence and Security, February 2017

The Global Risks Report 2018
World Economic Forum, February 2018

No meeting of minds in Munich over cyberattacks
Carnegie Europe, February 2018

Cyber-diplomacy: The making of an international society in the digital age
Egmont, January 2018

Cybersecurity of nuclear weapons systems: Threats, vulnerabilities and consequences
Chatham House, January 2018

Cyber mercenaries and the crisis in Ukraine
Council on Foreign Relations, January 2018

Reforming the U.S. approach to data protection and privacy
Council on Foreign Relations, January 2018

'Mind hacking': Information warfare in the cyber age
Istituto per gli Studi di Politica Internazionale, January 2018

Cyber threats to democratic processes
Institute for National Security Studies, December 2017

EU–NATO cybersecurity and defense cooperation: From common threats to common solutions
German Marshall Fund, December 2017

Asian cybersecurity futures: Opportunity and risk in the rising digital world
Observer Research Foundation, December 2017

Grid security is national security: Cyber threats to energy infrastructure and cities
Chicago Council on Global Affairs, December 2017

Democracy's eleventh hour: Safeguarding democratic elections against cyber-enabled autocratic meddling
Finnish Institute of International Affairs, November 2017

Main cyber threats now coming from governments as "state actors"
European Institute, November 2017

Cheap havoc: How cyber-geopolitics will destabilize the Middle East
German Marshall Fund, November 2017

The future of EU Defence: A European space, data and cyber agency?
Istituto Affari Internazionali, October 2017

Future war NATO? From hybrid war to hyper war via cyber war
GLOBSEC Policy Institute, October 2017

The defence-security nexus: Towards an EU collective security
European Political Strategy Centre, October 2017

Raising the consequences of hacking American companies
Center for Strategic and International Studies, October 2017

Democracy and cybersecurity
Brookings Institution, September 2017

Digital disinformation: A primer
Atlantic Council, September 2017

Controlling chaos: How Russia manages its political war in Europe
European Council on Foreign Relations, September 2017

Europol: The internet organised crime threat assessment (iOACTA) 2017
The Hague Security Delta, September 2017

The UN GGE is dead: Time to fall forward
European Council on Foreign Relations, August 2017

Strengthening the EU's resilience in the virtual domain
Wilfried Martens Centre, August 2017

Weeding out fake news: An approach to social media regulation
Wilfried Martens Centre, August 2017

EU cyber diplomacy requires more commitment
Clingendael, August 2017

Globally, people point to ISIS and climate change as leading security threats: Concern about cyberattacks, world economy also widespread
Pew Research Center, August 2017

Good neighbors make good security: Coordinating EU critical infrastructure protection against cyber threats
GLOBSEC Policy Institute, August 2017

Making Europe a data economy: A new framework for free movement of data in the digital age
Lisbon Council, July 2017

Cyber attacks: Understanding the basics
European Council on Foreign Relations, June 2017

The great unravelling: Four doomsday scenarios for Europe's Russia policy
Carnegie Endowment for International Peace, June 2017

Cybercrime and the digital economy in the GCC countries
Chatham House, June 2017

Building an effective European cyber shield: Taking EU cooperation to the next level
European Political Strategy Centre, June 2017

Why we need a Transatlantic charter for data security and mobility
Chatham House, June 2017

Meeting the Russian hybrid challenge: A comprehensive strategic framework
Atlantic Council, May 2017

Advancing human security through artificial intelligence
Chatham House, May 2017

Can Europe deal with cyberattacks?
Carnegie Europe, May 2017

Europe's digital power: From geo-economics to cybersecurity
European Council on Foreign Relations, April 2017

The enemy has a voice. Understanding threats to inform smart investment in cyber defence
New America Foundation, February 2017

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.

eprs@ep.europa.eu
http://www.eprs.ep.parl.union.eu (intranet)
http://www.europarl.europa.eu/thinktank (internet)
http://epthinktank.eu (blog)