Briefing
What Think Tanks are thinking
3 February 2017

European Parliament

Cyber-security

Allegations of interference in the US electoral campaign in 2016 through cyber espionage and leaks have put the spotlight on cyber-security and cybercrime, not only for ensuring financial or strategic advantages, but increasingly as means of pursuing political aims. As digital technologies grow in importance, the clear view among analysts is that cyber-crime is becoming a major threat to governments, businesses and societies as a whole.

This note offers links to **reports and commentaries from some major international think tanks and research institutes** on cyber-security and related issues.

Connectivity wars
European Council on Foreign Relations, January 2017

Trump must stand up to Russian cyberattacks
Atlantic Council, January 2017

The privacy paradox II: Measuring the privacy benefits of privacy threats
Brookings Institution, January 2017

Cybersecurity in the next administration
Hoover Institution, January 2017

Tackling cybercrime: Time for the GCC to join global efforts
Chatham House, December 2016

Russia's new information security doctrine: Guarding a besieged cyber fortress
Finnish Institute for International Relations, December 2016

Piratages informatiques aux Etats-Unis: Vers une cyberguerre froide?
Institut des relations internationales et stratégiques, December 2016

Medium-sized states in international cyber security policies
Clingendael, December 2016

Spotlight on Cyber VI: Respecting the digital Rubicon: How the DoD should defend the U.S. Homeland
Council on Foreign Relations, December 2016

Russia's old tricks against new targets
Atlantic Council, December 2016

Author: Marcin Grajewski, Strategy and Coordination Unit

The U.S. continues to face cyber threats in 2016
Heritage Foundation, December 2016

Cyber security in Singapore
Rajaratnam School of International Studies, December 2016

The defence of civilian air traffic systems from cyber threats
Instituto Affari Internazionali, December 2016

A lack of cybernorms threatens Western democracies
Carnegie Europe, December 2016

Pushing back on Russian meddling in Western elections
Carnegie Europe, December 2016

Cybersecurity and democracy: Hacking, leaking and voting
European Union Institute for Security Studies, November 2016

A framework for exploring cybersecurity policy options
Rand Corporation, November 2016

How to save election technologies from "hanging chads" and software malfunctions
Brookings Institution, November 2016

EUnited against crime: Improving criminal justice in European Union cyberspace
Instituto Affari Internazionali, November 2016

Creating a federally sponsored cyber insurance program
Council on Foreign Relations, November 2016

Lawful hacking and the case for a strategic approach to "Going Dark"
Brookings Institution, September 2016

Space, the final frontier for cybersecurity?
Chatham House, September 2016

Foreign policy instruments to increase future cybersecurity
Clingendael, August 2016

Due diligence and the futility of creating norms in cyberspace
Friends of Europe, August 2016

Cyber attacks go beyond espionage: The strategic logic of state-sponsored cyber operations in the Nordic-Baltic region
Finnish Institute for International Relations, August 2016

Building a comprehensive strategy of cyber defense, deterrence and resilience
German Marshall Fund, July 2016

Le secteur énergétique exposé à la cyber-menace
Institut français des relations internationales, July 2016

China and cyber: Attitudes, strategies, organisation
NATO Cooperative Cyber Defence Centre, June 2016

Is NATO Ready to cross the Rubicon on cyber defence?
NATO Cooperative Cyber Defence Centre, June 2016

Cyber attacks blurring borders between war and peace
Council on Foreign Relations, June 2016

Due diligence in cyberspace
Stiftung Wissenschaft und Politik, May 2016

Combatting cyber threats: CSIRTs and fostering international cooperation on cybersecurity
Centre for International Governance Innovation, December 2015

What Obama did and did not accomplish in cyber-espionage talks with Xi
Peterson Institute for International Economics, October 2015

Should US tech companies share their "source code" with China?
Peterson Institute for International Economics, October 2015

US-China cybersecurity agreement: A good case of cyber diplomacy
Egmont, October 2015

The danger of proliferating covert cyber operations
Clingendael, September 2015

The threat of state-sponsored industrial espionage
European Union Institute for Security Studies, June 2015

The dark side of the web: ISIL's one-stop shop
European Union Institute for Security Studies, June 2015

Cyber Jihad in the service of the Islamic State (ISIS)
Institute for National Security Studies, April 2015

Cyber-liberty depends on cyber-security
Fraser Institute, March 2015

Economic aspects of national cyber security strategies
NATO Cooperative Cyber Defence Centre, 2015