HEINRICH BÖLL STIFTUNG
The Green Political Foundation

Co-funded by the
Europe for Citizens Programme
of the European Union

US-China cybersecurity agreement: a good case of cyber diplomacy

Published on 30. September 2015 by Thomas Renard

The US and China concluded a major cybersecurity agreement during President Xi Jinping's visit to Washington, on 25 September. The agreement states that both sides will not engage in cyber-enabled economic espionage against each other or support such activities, and that they will take the necessary actions to curb and cooperate on cybercrime issues. Both sides also endorsed the latest report of the United Nations Group of Governmental Experts on Information Security (GGE), which marked itself a mild progress in global cooperation on cyber issues.

The US-China agreement may not be a game changer, but it is a positive step forward in a very sensitive policy area. Cybersecurity (in a broad sense) has been one of the major irritants in the bilateral relationship between Beijing and Washington. Over the past few years, the US has regularly accused China of committing hostile cyber acts. In May 2014, the US Department of Justice went as far as charging five Chinese military personnel for 'computer hacking and cyber espionage', whereas Barack Obama was preparing to impose sanctions against Chinese companies accused of intellectual theft, just a few days ahead of Xi Jinping's visit. In turn, China has expressed 'grave concern' following Edward Snowden's revelations of US cyber espionage. Clearly, distrust dominates this relationship.

In this context, it is needless to say that the bilateral agreement was the result of intense diplomatic efforts, including a four-day meeting between senior officials earlier this month. Furthermore, the agreement establishes two cooperation mechanisms that should facilitate exchanges and cooperation between Washington and Beijing. One such mechanism is a 'senior experts group' to discuss norms of behaviour in the cyberspace, whereas the other mechanism is a 'high-level joint dialogue' on cybercrime, meeting twice a year, 'to review the timeliness and quality of responses to requests for information and assistance with respect to malicious cyber activity of concern identified by either side'.

The rising importance of cyber diplomacy

The US-China cyber security agreement is a good illustration of so-called 'cyber diplomacy', which can be defined as the use of traditional diplomatic instruments to address cyber issues, such as cybercrime, cybersecurity or internet governance. Like any other form of diplomacy, it takes place both at the bilateral level and in a multilateral context, and it is underpinned by both informal meetings and institutionalised dialogues.

Cyber-diplomacy must be distinguished from 'e-diplomacy', which is characterised by the use of new technologies for broader diplomatic purposes. However, these two concepts belong to a broader category, 'digital diplomacy', defined as the conduct of diplomacy in the digital age – where the digital sphere creates the context, object and instruments of diplomacy.

Cyber-diplomacy is not entirely new. Already in the 1990s, states were arguing over the governance of the internet, notably in the context of the set-up of the Internet Corporation for Assigned Names and Numbers (ICANN), the multi-stakeholder body regulating the internet. Over the past few years, however, cyber issues have become so critical to the good functioning of modern societies, economies and governments that cyber diplomacy is no longer optional for global powers. As a transnational domain par excellence, cyber issues require states to cooperate in order to ensure their cyber security and prosperity (which is undermined by cybercrime and cyber economic espionage).

A number of bilateral cyber agreements, such as the one between the US and China, have been concluded recently to do just that. In another instance, the US and Japan agreed to deepen their cooperation on cyber defence last May. A few days earlier, China and Russia had pledged not to carry out cyber attacks against one another, while promising more cooperation on cyber security. A number of discussions also take place at the multilateral level, for instance in the context of the 'London process', which discusses cyber norms, as well as in the UN or GX systems. Overall, the fabric of cyber diplomacy is thickening quickly, as cyber issues become more central to global powers' foreign policy priorities.

Cyber Europe

The rising importance of cyber diplomacy is visible in Europe as well. A number of European countries are particularly active in this area, notably France and the UK. The European Union itself has developed a cyber security strategy in 2013, as well as guidelines for its cyber diplomacy in February 2015. These guidelines identify five main areas of action: promotion and protection of human rights in cyberspace; norms of behaviour and application of existing international law in the field of international security; internet governance; enhancing competitiveness and prosperity; as well as capacity building and development.

In order to pursue these objectives, the EU has deepened its cooperation with a number of countries, notably establishing structured dialogues on cyber issues (see also here). It has also been active in debates on internet governance, and in the promotion of multilateral instruments against cybercrime, such as the Council of Europe's Budapest Convention or the Global Alliance against Child Sexual Abuse Online (which was initiated jointly by the EU and the US). It also seeks to strengthen its digital growth through strategic partnerships, as illustrated by the EU-China agreement on 5G technology that was signed this week.

Overall, however, the EU's cyber diplomacy remains under-developed and under-delivering. The EU-US cyber partnership was the only one singled out in the 2013 strategy and certainly the most productive one by far. This is not entirely surprising, since the EU is both a fledgling cyber security and diplomatic agent. Yet, as cyber issues become increasingly central to global politics, and in light of the major US-China agreement, the EU cannot afford to remain on the sideline. It

must actively seek to shape the cyber agenda, both at the bilateral and multilateral levels. This, of course, cannot be done without full cooperation from its Member States.