Negotiating Order in Cyberspace: Choosing Economic Governance Over Security Spirals

Catherine Laporte-Oshiro and James Shires
Brussels Forum 2016 Young Writers Award Winners

Introduction

On 25 September 2015, Presidents Barack Obama and Xi Jinping reached a historic bilateral agreement on cyber-espionage.[1] A month later, the US-China "common understanding" was followed by a matching text agreed by President Xi and British Prime Minister David Cameron, as well as similar discussions between Chinese Premier Li Keqiang and German Chancellor Angela Merkel.[2] The rise of cyber-security on international agendas is unsurprising. A 2014 report by the Center for Strategic and International Studies, in partnership with antivirus firm MacAfee, put the global cost of cybercrime and cyber-espionage between $375 billion and $575 billion annually.[3] Senior US intelligence officials have explicitly named cyber-espionage as the highest national security threat they face.[4] These cyber agreements therefore have significant implications for transatlantic cooperation in an increasingly multipolar world.

Moreover, this cascade of collaboration suggests a gradual emergence of what Joseph Nye calls cyber norms or "rules of the road",[5] in contrast to earlier depictions of cyberspace as the "Wild West". While agreeing that these are certainly attempts to move beyond disorder, this paper argues that we now face a crucial choice. The subject of these agreements currently straddles two broad areas of foreign policy: national security and international trade. We argue that if the default approach remains one focused on national security, then spiraling threat perceptions and tensions will be the result, at serious cost to the US and EU, transatlantic cooperation, and global stability. However, if we can further incorporate these agreements into international trade practices, then a fragile global market which brings advantages to many has a better chance of succeeding. To use Nye's analogy, we need not only agree on the rules of the road, but also to check the map: are we going down the right road in the first place?

---

[1] Ellen Nakashima and Steven Mufson, "U.S., China Vow Not to Engage in Economic Cyberespionage", *The Washington Post*, September 25, 2015, accessed December 11, 2015, https://www.washingtonpost.com/national/us-china-vow-not-to-engage-in-economic-cyberespionage/2015/09/25/90e74b6a-63b9-11e5-8e9e-dce8a2a2a679_story.html.

[2] HMGovernment, "UK-China Joint Statement 2015," October 22, 2015, accessed December 1, 2015, https://www.gov.uk/government/news/uk-china-joint-statement-2015; Stefan Nicola, "China Working to Halt Commercial Cyberwar in Deal With Germany," *Bloomberg*, October 29, 2015, accessed December 1, 2015, http://www.bloomberg.com/news/articles/2015-10-29/china-working-to-halt-commercial-cyberwar-in-deal-with-germany.

[3] "Net Losses: Estimating the Global Costs of Cybercrime" (Center for Strategic and International Studies, June 2014).

[4] Gus Taylor, "James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to U.S.," *The Washingtion Times*, February 26, 2015, accessed October 28, 2015, http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/.

[5] Joseph S. Nye, "International Norms in Cyberspace," *Project Syndicate*, May 11, 2015, http://www.project-syndicate.org/commentary/international-norms-cyberspace-by-joseph-s--nye-2015-05.

1. Diagnosing Disorder: National Security or Economic Advantage?

The US and China agreed on 25 September that "neither country's government will conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors."[6] Behind this sentence, and its UK copy, lies a nascent distinction between different types of state action in cyberspace: on one hand, 'legitimate' national security espionage, which is not covered by the agreement and, on the other, 'illegitimate' economic theft, which is. Both are often described using the umbrella term 'cyber-espionage'.

This distinction has been stressed repeatedly by the US government. On one side, the US Federal Bureau of Investigations has indicted Chinese individuals who obtain foreign companies' trade secrets for the Chinese state. On the other, when many sensitive records were taken from the Office of Personnel Management, US officials acknowledged that it was a legitimate national security target, and the US is well known for its own cyber espionage capabilities.[7] Thus, the US maintains that the former is less internationally acceptable than the latter, even if both entail significant national costs and political challenges. However, this distinction is difficult to maintain, for four reasons.

First, the traditional US and European national security sectors, along with their amorphous 'critical national infrastructures', are highly privatised. Many companies are big economic *and* security players and therefore make attractive targets on both economic or national security terms. To take an extreme example, information about the US F-35 Joint Strike Fighter (JSF) was reportedly obtained by China through cyber-espionage in 2009, and China has recently unveiled a very similar plane.[8] This activity has clear security implications, in that China is now better able to match or disrupt US forces in a combat scenario. However, it could also be economically motivated, as China has its own security contractors, and developing a fighter jet is expensive and US defence firms have the most advanced technology. Additionally, defence and intelligence contractors are intimately involved in offensive, as well as defensive, cyber activity. The idea of national security cyber activity as being somehow 'state-on-state' is therefore inaccurate, making the separation of national security and fair economic competition difficult.

Second, the skills required for cyber investigation, and the economics of the cyber-security industry, also pull against this distinction. Cyber investigation requires extensive technical expertise, and uses unique terminology: exfiltration, intrusion, advanced persistent threat, and so

---

[6] Nakashima and Mufson, 2015.
[7] Ellen Nakashima, "U.S. Decides against Publicly Blaming China for Data Hack," *The Washington Post*, July 21, 2015, https://www.washingtonpost.com/world/national-security/us-avoids-blaming-china-in-data-theft-seen-as-fair-game-in-espionage/2015/07/21/03779096-2eee-11e5-8353-1215475949f4_story.html.
[8] Marcus Weisgerber, "China's Copycat Jet Raises Questions About F-35," *Defense One*, September 23, 2015, accessed December 10, 2015, http://www.defenseone.com/threats/2015/09/more-questions-f-35-after-new-specs-chinas-copycat/121859/.

on. The shared training of those in the national and commercial cyber-security sectors means actors like former National Security Agency director Keith Alexander move between the two easily, and use the same specialised language in both. This professionalisation of cyber-security across the public-private divide can be beneficial to those involved – the weight of national security issues sells cyber-security products, and the market value of government-developed skills and tools is broadly recognised – but it further blurs the line between security-focused states and market-driven corporations.

Third, the distinction is challenged by the difficulty of clearly *attributing* hostile cyber activity, and ascertaining the *intent* behind it. The attribution problem is well-captured by the broad phrase, "conduct or knowingly support cyber-enabled theft of intellectual property", in the US-China agreement. Not all cyber activity originating in China is performed directly by the government, or can be traced back to it. Criminals, hacking groups, and companies can all act as intermediaries; indeed, cyber activity is often deliberately conducted at 'arm's reach' from decision-makers. Finally, even when an intrusion is detected and initially attributed, the intent can still be uncertain – its purpose could be theft, espionage, contingency planning, data deletion, or a combination of several.

Fourth, the security-economic distinction challenges a widening view of security. This trend goes back to the Cold War and has been reinforced by recent financial crises, stretching definitions to include human, societal, and economic issues within a security paradigm. For example, the UK National Security Strategy sets out the activities of the defence and intelligence agencies using the concepts 'national security', 'economic security', and even 'national economic security'.[9] When the two concepts elide, as in that document, separating state-level economic advantage gained through hostile cyber activity from the national security threat posed by that activity becomes almost impossible.

Consequently, although the agreements carefully avoid security language, they are fighting against a larger tide, in which the organisations, politicians, and experts that deal with cyber issues frame them within a world of enmeshed economic advantage and national security. Depending on your perspective, the agreements become either an ineffectual hedge, or a deeper hypocrisy, where the fiction of a separation between economic advantage and national security in cyberspace benefits many of those involved. Merely leaving the word 'security' out of the text of international agreements does not work. Thus, the emerging agreements on cyber-espionage rest on a nascent distinction between state-backed cyber activity for national security and economic advantage, but this emerging norm is drowning in a broader sea of national security expansionism. The options are to either give up and return to a security frame or firmly commit to the security-economic distinction.

2. Security Spirals or Trade Foundations

[9] HMGovernment, "A Strong Britain in an Age of Uncertainty: The National Security Strategy" (London, UK: 2010).

The choice is clear. We now briefly explain how the institutional instinct towards national security raises the barriers against transatlantic cooperation, and then turn to the promising alternative: the international trade framework. We therefore move from diagnosing the underlying disorder behind the recent cyber agreements, to specific policy recommendations for going beyond this disorder.

The main barrier to cooperation in the security arena is a lack of international institutional competence. In Europe, the main vehicle for international cooperation is the EU, which does not include national security issues in its remit. While there is extensive European and transatlantic security co-operation on some national security issues – whether through formal organisations such as Europol and Interpol, or through multilateral relationships between relevant domestic agencies – this co-operation focuses on issues such as terrorism and organised crime, or peacekeeping interventions. Hostile state activity is much more difficult to incorporate into such formats.

A potential vehicle for transatlantic cyber cooperation is through the North Atlantic Treaty Organisation (NATO). At first sight, this seems promising: the NATO cyber-security centre has produced influential works on international law in cyberspace – the 'Tallinn manual' – and has recently incorporated cyber-security into its 'Emerging Security Challenges'. However, NATO's focus, understandably, is on large-scale cyber-attacks like those attributed to Russia in Georgia and Estonia rather than lower-level, but more common, hostile cyber-activity. More problematically, there is another institutional arrangement highly influential in cyber-security, known as "Five Eyes", which only includes the US, UK, Canada, Australia and New Zealand. The prominence of the Five Eyes in cyber-security – and the sensitivity of the sources and techniques informing their perspective on those issues – means that pan-European cooperation on economic cyber activity is unlikely as long as it falls primarily in the security sphere.

As well as institutional barriers to cooperation in security, there are more pervasive problems. Treating cyber intrusions as a national security issue inflates the risks by placing them in the same realm as war and terrorism. This leads to a rhetorical security spiral up the risk scale. For example, in a recent speech at the UK signals intelligence agency, GCHQ, UK Chancellor George Osborne elided economic theft, where the UK's "starting point must be that every British company is a target", and more serious security issues, by immediately talking about ISIL's attempts to build deadly infrastructure-destroying capabilities.[10] This non-sequiteur was only logical due to the speech's location, because such agencies have a responsibility to consider and plan for worst-case scenarios, including cyberterrorism.

Furthermore, given that the problem of state-backed cyber theft, by definition, has a state at the other end, the primacy of security organisations also creates a different kind of spiral due to the signals it sends out. In the case of the US and China, the involvement of the PLA and the

[10] George Osborne, "Chancellor's Speech to GCHQ on Cyber Security," November 17, 2015, accessed November 20, 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security.

Department of Defense Cyber Command on each side suggests to the other that the worst-case scenario – the transformation of economic theft into potentially destructive activity – is more likely to be the case. Osborne's well-publicised visit to GCHQ also sends the same signal. More widely, the twin roles of GCHQ and the NSA in both information assurance (defensive activity) and intelligence collection, as well as their symbiotic relationship with the military, reinforces a security spiral on both sides.

To be clear, we do not want to suggest that there is no role for NATO, the Five Eyes, or other security organisations in cyber-security. Rather, our argument is that in order to meaningfully distinguish between state-backed economic theft in cyberspace and myriad other cyber-security issues, and in order to create Europe-wide and transatlantic cooperation on the former, their *primacy* must be reduced. What, then, is the alternative?

Amidst the language of war that clouds cyber issues today, we are forgetting that we have a far superior frame for handling them: trade. The international trade regime is arguably the most advanced form of global governance and has a proven track record of promoting prosperity and de-escalating tensions. Through a network of bilateral, plurilateral, and multilateral agreements, with the World Trade Organization at the centre, states have committed themselves to increasingly fair and open markets, lawful resolution of trade conflicts, and strong enforcement measures. This is not to say that the system is perfect or that all issues have been put to rest – far from it. However, it is a strong framework for constructive negotiation, thereby preventing security spirals and their economic equivalent, trade wars.

The trade framing has worked in the past for issues intimately connected to today's cyber-espionage, such as intellectual property (IP). In the 1990s, IP protections in China were scarce and, even when they did exist, rarely enforced. Like economic cyber espionage today, IP infringements at the time weakened the competitive position of American and European countries, economies, and, ultimately perhaps, militaries. The path of a security spiral was available, but instead the US, along with European allies, turned to trade negotiators. Although the problem is not solved, huge strides were made, including a series of IP agreements throughout the 1990s, culminating in China's WTO accession in 2001.[11]

The trade framing transforms the landscape of actors and interests. Economic issues tend to be more positive sum than security, and economic officials act accordingly, producing positive instead of negative spirals. Indeed, in the 1990s, liberal Chinese officials like Premier Zhu Rongji were looking for foreign allies and even a bit of pressure to use as leverage against conservative rivals in order to push through economic reforms.[12] Thus, trade negotiations, with their combination of market-access carrots and sanction sticks, can be very effective at dealing with non-competitive behavior and preventing escalation.

---

[11] James K. Sebenius and Rebecca Hulse, "Sequencing, Acoustic Separation, and 3-D Negotiation of Complex Barriers: Charlene Barshefsky and IP Rights in China," *International Negotiation* 8 (2003): 311–38.
[12] Joseph Fewsmith, "The Political and Social Implications of China's Accession to the WTO," *The China Quarterly*, no. 167 (2001): 573–91.

3. Policy Proposal: Trading in Cyber's Security Framing

Today, the trade approach can be just as effective for economic cyber issues. Rather than painting cyber attacks as an existential security threat and pulling ourselves into a spiral of conflict, we can place them under the domain of our economic agencies. Such a change would transfer primacy on the issue away from security actors in China, Europe, and the US and place it in the hands of more liberal, pro-engagement officials in all three. In a trade framing, everyone can reap gains from cooperation: Western companies get better IP protection, but so do Chinese companies, and President Xi gets an international push for his economic reform agenda. Additionally, the trade framing of cyber security could promote greater inter-EU and even US-EU cooperation, as the European Commission has exclusive competency in trade issues. Finally, trade is an area where disagreements can lead to constructive negotiation, and the European focus on data privacy or the Chinese use of state intervention in markets are areas where the US could learn a thing or two.

It is tempting to beat the drums of war on cyber, with difficulties in attributing attacks and fears that come with technological change and rising powers; however, such a path leads ever downward into conflict. Thus, we propose that economic-related cyber issues be made the domain of US Trade Representative (USTR) and the EU Directorate General for Trade (DG TRADE), and funding, expertise, and intelligence should be redirected to reflect that shift. From the US Cyber Command's $5.5 billion annual budget, $500 million should be reallocated to a new USTR economic cyber unit, and DG Trade should receive $300 million.[13] These funds should be used to re-hire and train personnel, not only in cyber-related skills but in an economic approach to cyberspace as well. For example, rather than 'espionage,' we should speak of 'infringement.' Cyber information sharing can piggy-back on existing international networks of economic officials, who already coordinate responses to barriers to trade or treaty enforcement issues, rather than Five Eyes-style intelligence procedures.

The trade framing is not an immediate fix, and it will not work for all cyber issues, including more traditional state-to-state espionage and offensive military capabilities. However, this shift will set us on the road of international dialogue and cooperation. We have too much to lose by claiming cyberspace as part of the anarchic security landscape, and so much to gain from negotiating them under the international economic order.

---

[13] Aliya Sternstein, "The Military's Cybersecurity Budget in 4 Charts," *Defense One*, March 16, 2015, http://www.defenseone.com/management/2015/03/militarys-cybersecurity-budget-4-charts/107679/.