European Union Studies Association

15th Biennial Conference – Miami, Florida

Transatlantic cybersecurity cooperation: a new issue area for the transatlantic community?

**[DRAFT/WORK IN PROGRESS – PLEASE DO NOT CITE]**

Author:

Dr. Dimitrios Anagnostakis

Teaching Fellow at Liverpool Hope University (UK)

E-mail: dimitriosanagnostakis@gmail.com

Abstract:

Inequalities in terms of military and power capabilities have allegedly led countries such as China, Iran, and Russia to pursue disruptive cyber attacks against the West. Such cyber attacks, along with terrorism, have been described as the "weapons of the weak". In the face of this threat the West has tried during the last years to coordinate its efforts and to benefit from shared experiences and practices. This paper seeks to investigate the extent to which the emergence of new cybersecurity threats has produced a new collective transatlantic identity based on common threat perceptions and interests. In other words, this paper looks whether and how the transatlantic security community has been invigorated by the emergence of this new issue-area of cooperation. This paper also examines the transatlantic actors’ principles, norms, rules, and decision-making procedures in the issue area of cybersecurity. Regarding the paper's theoretical framework, this research builds on the security communities approach and the constructivist framework which focus on shifting identities and on how cooperation can lead to the construction of a common identity as well as on insights from regime theory.

**Introduction**

This paper identifies a number of issues related to transatlantic cybersecurity that have recently emerged.

Transatlantic cooperation on internal security issues has been intensified since the 9/11 terrorist attacks. This issue-area comprises of the policies and measures that states and regional and international organisations adopt and employ to combat and address internal security threats. The internal security threats can range from organised crime, terrorism, and drug trafficking to cyber-crime, human trafficking and illegal immigration (Rees and Mitsilegas et al. 2003: 2; Rees 2006a 6). Regarding the EU, the Council of the EU identified in 2010 in EU’s first internal security strategy “terrorism, serious and organised crime, drug trafficking, cyber-crime, trafficking in human beings, sexual exploitation of minors and child pornography, economic crime and corruption, trafficking in arms and cross-border crime” (Council of the EU, 5842/2/10 2010: 2) as significant challenges to the internal security of the union and its member states. The tools that the Council suggested for addressing the above threats included judicial cooperation (for instance, the mutual recognition of judicial decisions and joint investigations), the sharing of information (for example, the establishment of a passengers’ data sharing system), customs cooperation, and border controls and the integrated management of external borders. Similarly, the communication from the Commission in 2010 (European Commission COM 673 2010) regarding the implementation of EU’s internal security strategy identified terrorism, organised crime, cyber-crime, natural and man-made disasters and the management of external borders as the main internal security challenges of the EU; the Commission called, among others, for the establishment of an EU PNR system, the expansion of risk-management techniques for customs controls in member states, and the intensification of judicial and law enforcement cooperation.

The above internal security threats and measures were also highlighted in the US strategic documents. For instance, in the US “Strategy to Combat Transnational Organized Crime” (2011) the US highlighted, among others, the threats of drug and human trafficking and the measures and tools of intelligence sharing, targeting the financing of organised crime, and strengthening the judicial and law enforcement cooperation with third partners and international organisations, such as Europol and Interpol. Additionally, the US “National Strategy for Homeland Security” (2007) emphasised the threats of terrorism and natural and man-made disasters and focused on tools such as border controls, customs security measures and international cooperation.

Given the above, internal security is a policy area that comprises of police and law enforcement measures, judicial tools, intelligence, border and transportation security, and critical infrastructure and civil protection measures. The above tools and measures are used for addressing internal security challenges, which include terrorism, organised crime, drug trafficking, illegal immigration, human trafficking, and cyber-crime. In this sense, internal security overlaps with the concept of homeland security, which is preferred in the US (Dalgaard-Nielsen 2006: 1) and which comprises of “intelligence, justice and law enforcement, border and transportation security, infrastructure protection, counter-CBRN (Chemical Biological Radiological and Nuclear) measures, detection, early warning, antiterrorism research, and emergency preparedness and response” (Dalgaard-Nielsen 2006: 3). Similarly, both concepts are broad in terms of the scope of the threats and challenges they seek to address (Dalgaard-Nielsen 2006: 2; House of Lords Paper 149: 11).

Transatlantic cooperation on internal security matters emerged after the 9/11 attacks and it was focused mainly on the sub-areas of law enforcement, judicial cooperation and border and transportation security. This reflected the fact that in the aftermath of the 9/11 attacks the EU was more active in the fields of judicial and law enforcement cooperation that it was in the fields of civil and critical infrastructure protection or emergency response. In particular, the EU and the US have signed a number of agreements on customs security, the transfer of air travellers’ data, the transfer of financial data, mutual legal assistance and extradition, security research, and the cooperation and information sharing between the US and Europol and Eurojust.

**Transatlantic cybersecurity: issues for consideration**

**1) Threat perceptions and principles: common or diverging?**

In the literature on transatlantic counter-terrorism cooperation diverging threat perceptions have been often cited as a factor that can create friction between Europeans and the Americans. The first wave of transatlantic counter-terrorism literature focused on evaluating the prospects for cooperation in this policy area. The main issue that was examined under this context was the two sides’ threat perceptions and their impact on cooperation. This literature discussed the questions of whether the US and Europe had common interests and common threat perceptions with regard to terrorism, whether their respective responses and tools differed and how differences could impede cooperation (Keohane 2005; Neuhold 2006). In particular, Stevenson (2003) and Shapiro and Byman (2006) talked about a ‘continental drift’ and a ‘transatlantic counter-terrorism gap’ respectively, in the sense that, the US and Europe faced different threats, and therefore their interests diverged. The US was the main target of al-Qaeda while European states were the aim of smaller and less dangerous local and regional groups. Stevenson (2003) also highlighted the different historical experiences that Europe and the US had with regard to terrorism. For Europe terrorism was a domestic problem and therefore the solutions that were chosen came from the law-enforcement arsenal of the state. For the US terrorism was predominantly an overseas issue and as a result, it was argued, that the solutions tended to focus on military and foreign policy tools.

Rees (2006a; 2006b; 2011) and Rees and Aldrich (2005) talked about the different strategic and counter-terrorism cultures of the two sides and about the US conceptualisation of terrorism as a problem linked with the issue-areas of weapons of mass destruction and ‘states of concern’. Rees (2006a) and Keohane (2005), however, cautioned against this tendency to associate the US counter-terrorism response only with military measures and to ignore the broad array of law enforcement tools that the US has employed. From a similar historical perspective, Sloan (2003) and Neuhold (2006) noted that Europeans have experienced many instances of terrorism and therefore they have been more accustomed to vulnerability than the US. These different perceptions shaped the corresponding responses to the threat against terrorism. While the US adopted a policy of risk elimination the European states tended towards risk avoidance or risk management.

The above literature has overemphasised the differences between the two sides on counter-terrorism. The cooperation between the EU and the US on various areas of internal security ranging from travel documents and customs security to legal assistance and air passengers’ data disconfirmed the notion of a transatlantic counter-terrorism gap.

Similarly, in the case of cybersecurity the threat perceptions of the two sides are closer. In the EU cybercrime costs around 0.41% of GDP while in the US this cost is around 0.64% (Pawlak 2016). In terms of the official documents, EU’s cybersecurity strategy mentions that “threats can have different origins – including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes” (European Commission 2013). In other words, the Commission identifies cybersecurity threats in a broad way, including both the civilian and the military fields. Similarly, the US “International Strategy for Cyberspace” published in 2011 notes that the US will “defend its networks, whether the threat comes from terrorists, cybercriminals, or states and their proxies.”

At the same time, however, the US places more emphasis on building the capacity for retaliatory cyber-kinetic attacks which can cause physical damage or destruction while Europeans emphasise more the law enforcement aspect of cyber security. The 2015 “Department of Defense Cyber Strategy” mentions explicitly that the US will “respond to cyberattacks against U.S. interests at a time, in a manner, and in a place of our choosing, using appropriate instruments of U.S. power and in accordance with applicable law”. This transatlantic difference is similar with the previously identified pattern of the US emphasising more the military aspects of the fight against terrorism while Europeans and the EU focused on law enforcement and intelligence. It should be noted, nevertheless, that this description simplifies to some extent the reality of transatlantic cooperation.

In terms of principles, the EU and the US agree on a number of principles related to cyberspace and cybersecurity. First, both sides agree on preserving the open character of the internet and increasing the access to cyberspace. This principle differs from the approach of states such as Russia and China which are in favour of more restrictive policies with regard to internet and censorship in the cyberspace. In other words, the EU and the US are committed in maintaining the openness of the internet and safeguarding the current multi-stakeholder model.

Second, and related to the above, is the principle that protecting the fundamental freedoms and the free flow of information on the one hand and enhancing cybersecurity on the other hand are not mutually exclusive aims. While EU’s cybersecurity strategy states that cybersecurity can only be effective when it is based on fundamental rights and freedoms (European Commission 2013) the US strategy highlights that the US “policies flow from a commitment to both preserving the best of cyberspace and safeguarding” the American principles (The White House 2011). A similar principle unifies the EU and the US in the area of customs security where the two sides agree on the principle that trade facilitation should not compromise customs and container security and that on the contrary measures that promote customs security can have beneficial effects for trade (Anagnostakis 2016; Anagnostakis 2017).

Third, the cybersecurity strategies of both sides place huge emphasis on international cooperation and multilateral diplomacy. In other words, it is explicitly acknowledged by both the EU and the US that unilateral solutions are not only ineffective but they can also increase the costs for businesses which might have to comply with different sets of rules and regulations.

**2) The overlapping of different regimes**

In the current environment of global governance international regimes interact with each other and global rules often overlap with each other. Linkages may emerge between different regimes when the rules and regulations that are negotiated in order to address a certain issue or problem have ‘unintended consequences affecting other regimes’ (Young 1994: 25).

In the case of transatlantic relations data protection and the regional European data protection regime has often created friction in the relations between the EU and the US. In the past, the security rules that were negotiated between the two sides on issues such as the exchange of PNR information and the transfer of personal data from Europol to the US touched upon EU’s data protection regime.

Similarly, the EU has often expressed concerns that the US customs security measures might amount to non-tariff trade barriers affecting the international trade regime. The new roles envisioned for the private sector were accompanied by economic costs for the private companies which had to adapt their modes of operation and possibly invest in new infrastructure.

There is a possibility that transatlantic cybersecurity relations will be affected by this perennial issue of friction, namely data protection. EU’s cybersecurity mentions explicitly that any cybersecurity measure should be compliant with EU’s data protection law. This scenario should not be exaggerated however. The Commission officials responsible for internal security affairs are closer to the US positions that normally assumed in the literature, and in the past they have acknowledged the US position that the American data protection system although it is different from the European data protection regime it accords the same protections to individuals.

An additional example of overlapping regimes is the realisation that cybersecurity measures are linked with the issue of internet governance in general. In other words, any attempt to establish rules for cybersecurity touches upon the issue of how internet and cyberspace should be regulated. On this latter issue the EU and the US agree, both sides supporting the multi-stakeholder model and opposing the efforts of China and Russia to legitimise enhanced state intervention on cyberspace.

**3) The involvement of the private sector**

From a security governance perspective, researchers have focused on the shift from government to governance and on how states cooperate not only with other states but also with non-state actors, such as international organisations and private companies, for the provision of security (Krahmann 2005). In the case of customs, for example, the EU and the US suggested that the huge security gaps in international supply chains can be addressed by giving incentives to private companies in order they can adopt voluntarily certain security standards. These incentives took the form of the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Authorised Economic Operator (AEO) programmes in the US and the EU respectively. Similarly, in another case, that of the PNR agreements, the airlines would allow the US law enforcement authorities to access the booking information that the airlines had previously collected for commercial purposes.

Similarly, in the case of cybersecurity both sides agree that no measure can be effective without the active support of the private sector. In particular, the official strategies of both the EU and the US use the same language highlighting the shared responsibility of companies in the private sector.

A related concern for the private sector was the potential emergence globally of multiple and overlapping security standards which would mean that companies would have to comply each time with different sets of rules. Such fragmentation of global standards could create costs and inefficiencies for companies which operated globally.

**4) Socialisation processes and institutional settings**

EU and US officials meet regularly in a number of different institutional settings. First, the two sides have established the EU-US Working Group on cybersecurity as well as a similar group on cybercrime, and in these groups the EU and the US exchange and share best practices, technical expertise, and reflect on future measures and policies related to cybersecurity. In other words, these institutional settings can provide the necessary framework for the two sides’ socialisation and learning and the establishment of a common transatlantic epistemic community. A similar process takes place during the joint EU-US cyber-exercises which have been organised in the past and in which the two sides were able to test their response on different scenarios related to cyberattacks.

Additionally, the exchange of liaison officers between the EU and Europol on the one hand and the US on the other hand creates a similar potential for the exchange of expertise and better practices on cybersecurity. The more Europol acquired more powers and competencies in the past the more the US was interested in working with the agency. This was especially in the area of cyber-crime where Europol has conducted a number of successful operations, some of them together with the US. The fight against child pornography, banking fraud and identity theft were in particular some of the particular areas that Europol built expertise over the years. The recognition of the value of Europol for the US is reflected on the fact that as of 2013 seven US federal agencies had liaison officers in Europol’s headquarters.

The institutional links between the EU and the US are also important in terms of the operational cooperation on the fight against crime and terrorism. In particular, the EU and the EU member states have been keen in the past to use the EU-US mutual legal assistance as a tool in order to acquire from the US cyber evidence, given that the majority of data providers are located in the US. The huge number of requests for cyber evidence by Europeans has resulted in a clogging in the system with the result that the US tries to promote alternative means through which Europeans can access this information (for example through direct contacts between private companies and practitioners).

**5) Transatlantic cooperation on global standards for cybersecurity**

The security measures and standards that the EU and the US have negotiated and adopted in the past in areas such as customs security and PNR transfers could potentially serve as international models and be exported globally in the form of international standards. Similar processes of informal global standard-setting have been identified in the area of international intelligence liaison (Svendsen 2008; Svendsen 2011). Given that the EU and the US are the biggest and most influential actors in the field of internal security and counter-terrorism they could adopt a leadership role by engaging more actively with third states and international organisations. Through the combined weight of the EU and the US laggard states could be persuaded to implement counter-terrorism instruments and measures adopted by the United Nations or other organisations. The EU-US cooperation in establishing global standards could also be important for the avoidance of having overlapping and fragmented sets of rules which create costs and inefficiencies for companies and make international cooperation more difficult.

Therefore, it is important to examine to what extent the two sides cooperate and coordinate their positions on cybersecurity in international and multilateral for a or to what extent the EU adoption of the US rules legitimises them and makes easier their adoption by third countries.

**6) Cybersecurity as part of societal security**

Finally, given the recent and frequent allegations of Russia interfering and meddling with the elections in a number of Western states (e.g., the US Democratic Convention in 2016), it could potentially help to think of cybersecurity as part of the broader concept of societal security.

In particular, Esther Brimmer incorporates the concept of homeland security into “societal security” arguing that the former could be conceptualised as a subset of the latter. According to Brimmer, during the last decades the concept of security has evolved: the main focus of the transatlantic allies during the Cold War years was territorial defence while during the first decade after the end of the Cold War issues such as “backlash” states and humanitarian crises came into the forefront of the security agenda. Finally, the terrorist attacks of 9/11 highlighted the growing threat from asymmetric challenges and from non-state actors which had the ability not only to strike western targets abroad but also to strike “targets at home (…) at the core of the western system.” Brimmer notes that enemies such as Al Qaeda do not have any claims in resources or territories and that their aim is to erode and undermine western societies. From this follows that security is not only about defending territories but also about protecting “the values, connections, and infrastructure [that characterize] the modern globalized world.” Brimmer is thus in favour of a holistic approach to security or, as she names it, societal security. A holistic approach not only it includes efforts to prevent terrorist attacks, to reduce vulnerabilities and to minimise the consequences if attacks occur but it also incorporates the respect for and the protection of societal values such as the rule of law and civil liberties.

According to this line of thinking, societal security consists of two elements: cohesion and physical protection. Cohesion includes the values that characterise and bind a society: democracy, rule of law and civil liberties, education, welfare, and pluralism. Physical protection includes infrastructure, public health, natural disaster relief, environmental quality and anti-terrorism measures aimed at preventing attacks within the US. Answering the question of how does homeland security fit into that scheme Brimmer notes that homeland security includes components from both categories. In particular, the parts that are relevant for homeland security are rule of law and civil liberties from the “cohesion” category and infrastructure, public health, natural disaster relief and anti-terrorism measures from the “physical protection” category.

The above description of societal security is relevant for cybersecurity, especially given the fact that the EU and the US have already emphasised in their respective strategies that any cybersecurity policies and measures should not undermine fundamental rights and freedoms but rather support and strengthen them. In practice, therefore, and seen from this perspective of cybersecurity as part of a broader societal security framework, the Western cybersecurity measures that aim to stop and deter a potential Russian disinformation campaign should explicitly aim towards the support of the values that characterise and bind a society: democracy, rule of law and civil liberties, education, welfare, and pluralism.