Briefing

Perspectives on transatlantic cooperation

July 2016

European Parliament

Cybersecurity and cybercrime

Building more resilient and prosperous transatlantic societies

SUMMARY

Internet-based platforms are increasingly used for delivery of services, basic governance functions or communication. As such, open and secure access to Internet constitutes a significant element in generating growth, prosperity and citizens' empowerment on both sides of the Atlantic. However, this potential is increasingly undermined by digital risks and vulnerabilities in cyberspace: online fraud, attacks on critical infrastructure or the use of new technologies by terrorist networks. According to several studies, Europe and the United States can still reap tremendous benefits from digitisation but, in order to secure the potential gains, there need to strengthen transatlantic cooperation in building more resilient systems and societies, as well as deliver on their commitments to enhancing ties between regulatory, law enforcement, policy and civil society actors.

This briefing forms part of a broader research project on the perspectives on transatlantic cooperation in the US election year, requested by the Chair of the European Parliament's delegation for relations with the United States.

In this briefing:

EPRS | European Parliamentary Research Service

Author: Patryk Pawlak; Graphics: Christian Dietrich

Members' Research Service

PE 586.612

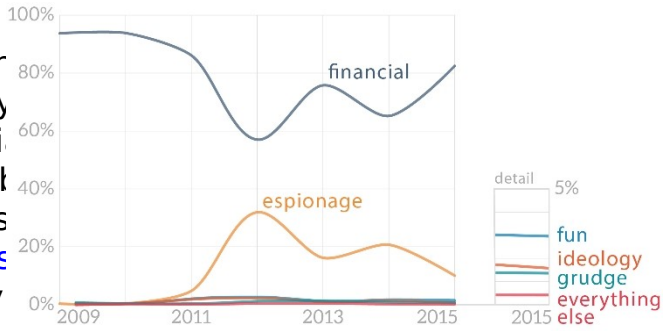
EN

Context and the state of play

In order to protect the positive impact of the internet on stimulating growth an creation, both sides of the Atlantic recognise the urgent need to strengthen the cooperation on eradicating safe havens and on building capacities to improve resilien of their systems and societies to criminal networks, cyber espionage and attack critical infrastructure (see Figure 1).

Firstly, improving cybersecurity reducing the effects of cybercrime in the transatlantic area is the protecting and further unlockir benefits of the digital economy Figure 2 and Figure 3). The reli of our societies on internet-b platforms for delivery of services and communications increases vulnerability to digital security According to existing studies, by 2025 internet-related technol such as mobile internet, the Internet of Things and cloud computing will generate potential economic benef between US$8.1 trillion and US$23.2 trillion annually. At the same time, the contribut of the internet economy to the global economy is between US$2 trillion and US$3 tril – up to 20% of this amount (US$400 billion) is lost due to cybercrime.

Figure 1 - Percentage of breaches (per threat actor)



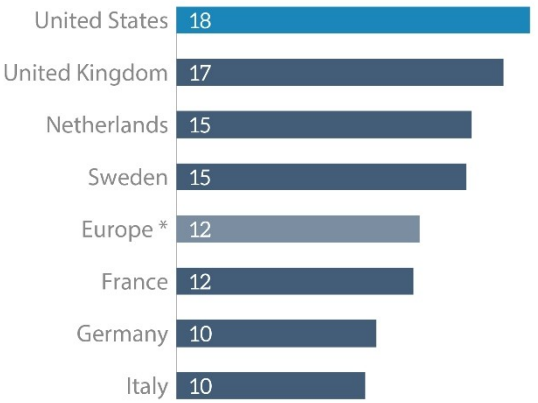
Data source: Verizon, 2015.

Secondly, the trends in online demographics suggest that the traditional leading role the EU and USA have played in shaping global standards and policies will increasingly challenged by emerging digital powers in Africa and Asia. The number of internet use expected to reach 4.7 billion by 2025, but most of this growth will come, not from the transatlantic area, but from developing countries and emerging economies, who citizens will represent 75% of the world's online population. For instance, while India experience growth of over 3 000% in the total number of broadband subscriptions 2025, reaching a total of 700 million people online, over the same period, the population in the transatlantic area will reach 565 million people.

Thirdly, all too often, regulatory approaches and policies adopted on each side of the Atlantic can turn the EU and the USA into each other's 'worst enemy' and distract the from the more significant threat posed by criminals, terrorists or other countries. This even more so in the post-Snowden world where the calls for a 'European stra autonomy' and the US claims of digital supremacy have become dominant in the poli discourse. The negotiations of the four EU-US Passenger Name Records (PNR) Agreements and the set back to transatlantic data exchanges resulting from the Cour Justice ruling in the *Schrems Case* (i.e. invalidating the EU-US Safe Harbour Agreemer teach us that *a priori* policy coordination and consultation between the EU and the US might be more effective than constantly placing the transatlantic relationship in a *pos factum* crisis management mode. This should not be the fate of cybercrime and cybersecurity cooperation. Because a 'transatlantic digital marketplace' cannot be bu on insecure and unstable foundations, these two policy areas cannot be viewed as a

another 'island of cooperation' in the transatlantic sea of initiatives and needs to be mainstreamed into regulatory discussions across the board.

Figure 2 - Share of digitisation potential realised (%)



* Weighted average of six countries that make up 60% of Europe's population and 72% of GDP

Figure 3 - Digital share of economy (%)

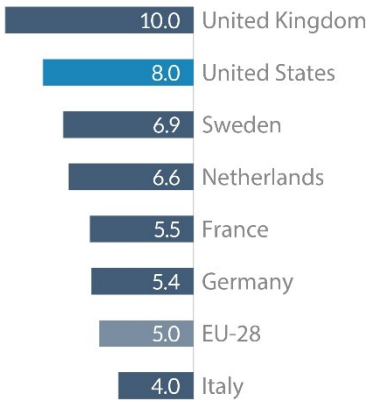
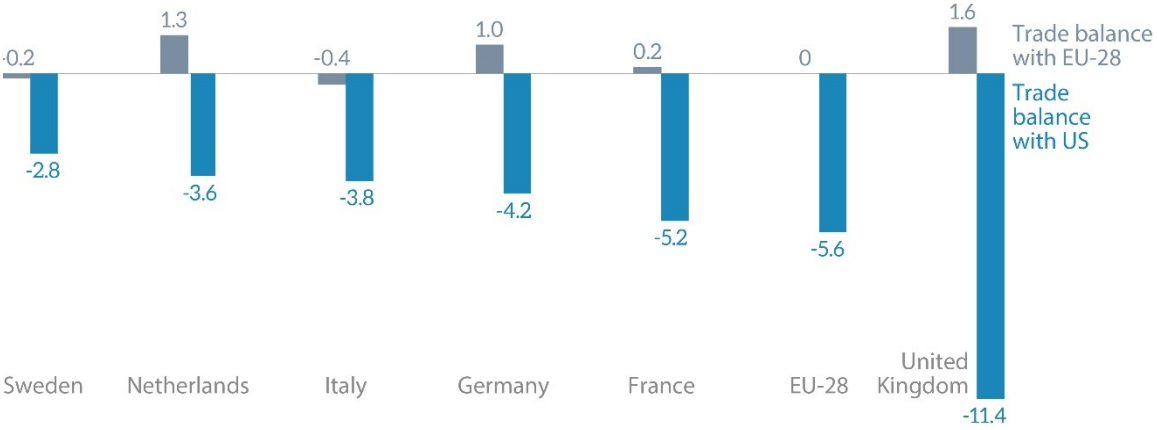


Figure 4 - Digital trade balance (% of total services trade with the US and the EU-28)



Data source for Figures 2, 3 and 4: McKinsey Global Institute, 2016.

A case for closer transatlantic cooperation

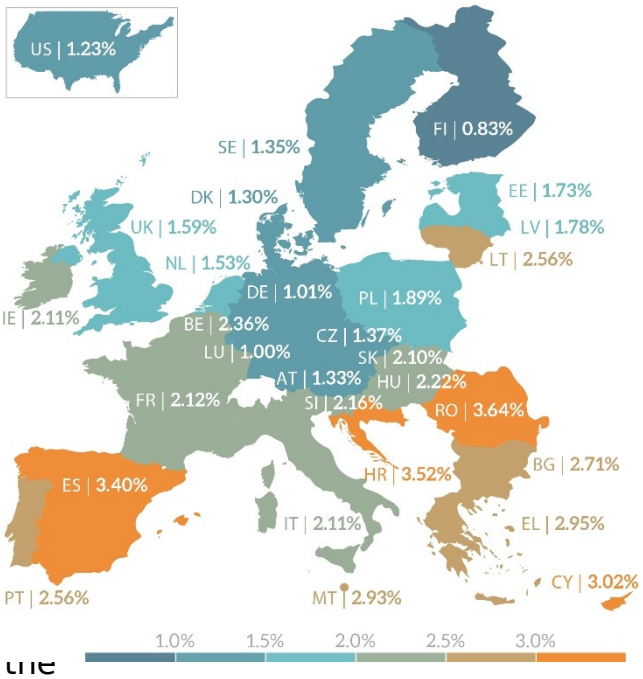
As the potential gains from attacks increase (be it either for common cyber criminals state sponsored groups) and the threshold for access to cyber-tools decreases (prima due to the development of the 'malware as a service' business), the threat to the EU US grows. This trend is accelerated by limited human, legal and institutional capacitie some regions of the world – in particular in Africa and eastern Europe, which facilitate the emergence of safe havens, from which criminal networks can harm citizen businesses operating in the EU and the US. Consequently, addressing cybercrime and building more robust cybersecurity is essential for the economic growth in the transatlantic area.

A cleaner and sustainable cyber ecosystem

One of the key problems in addressing cybersecurity is a limited understanding of glo 'cyber health' – or, in other words, conditions under which malicious activity and risk conditions spread in cyberspace. The unhealthy cyber ecosystem facilitates the cond of illicit activities in cyberspace (e.g. attacks on critical infrastructure, cybercrime) an

complicates the response (i.e. problems with attribution). By drawing the analogy with international responses to global health crises like malaria or this model points to the import of international cooperation in response (i.e. killing the viru cleaning up the infected compu and prevention (i.e. securing devices and educating users number of malware-infected ho in the EU and USA is relatively for some countries, given th world average is 16.9 compute 1 000 unique computers on malware was detected and removed (1.69%) (see Map 1). implies that the countries with the most infected computers ma easier for **cybercriminals** to s their piece of malware online.

Map 1 - Percentage of computers cleaned*



Data source: Microsoft, 2015.
*Computers with Microsoft real-time security products and the Malicious Software Removal Tool, 4Q2015.

Access to such computers can be purchased for small amounts: access to US-based h costs US$1 000 for 10 000 hosts and to EU-based hosts as little as US$400 for the sa number of hosts. As a result, up to 20% of US$3 trillion that the internet economy contributes to the global economy is lost due to cybercrime (US$400 billion). In the E the cost of cybercrime is estimated at 0.41% of GDP whereas in the US it is about 0.6 That translates into a potential loss of as many as 200 000 American and 150 000 European jobs due to cybercrime. A different study conducted regularly by the Ponem Institute estimates the average total **cost of a data breach** at US$3.79 million. In 2015, the cost for individual countries was between US$146 for Italy and US$217 for the Un States (Germany –US$211, France – US$186, UK – US$163). Nonetheless, the cost ha grown for all those countries since 2013.

Bigger and more resilient economic growth

There is a universal understanding that increasing internet connectivity contributes to economic growth – between 1 and 2% GDP growth for every 10% of the conne population. At the same time, there is still limited acknowledgment of the fact that cy insecurity constitutes an indirect **tax on growth**. The United States estimates the an impact of international intellectual property (IP) theft to the American economy US$300 billion – or 1% of its GDP. The United Kingdom, Netherlands and Germany hav registered similar estimated losses in GDP, which in times of slow economic growth is significant. That means that as the size of the 'digital economy cake' gets smaller due data breaches or attacks on critical infrastructure, so does the share of EU and US citi who could potentially benefit from it. According to some scenarios looking into to the possible effects of a large-scale cyber-attack on critical infrastructure, a cyber-attack the power grid in the north-eastern United States could cause an electricity blackout plunges an area covering 15 US states, including New York City and Washington DC, i darkness and leaves 93 million people without power. In addition to severe impact on

population (e.g. a rise in mortality rates as health and safety systems fail, and disrupt to water supplies as electric pumps break down), such an attack would cost the economy between US$243 billion and US$1 trillion.

Potential for convergence and/or joint action

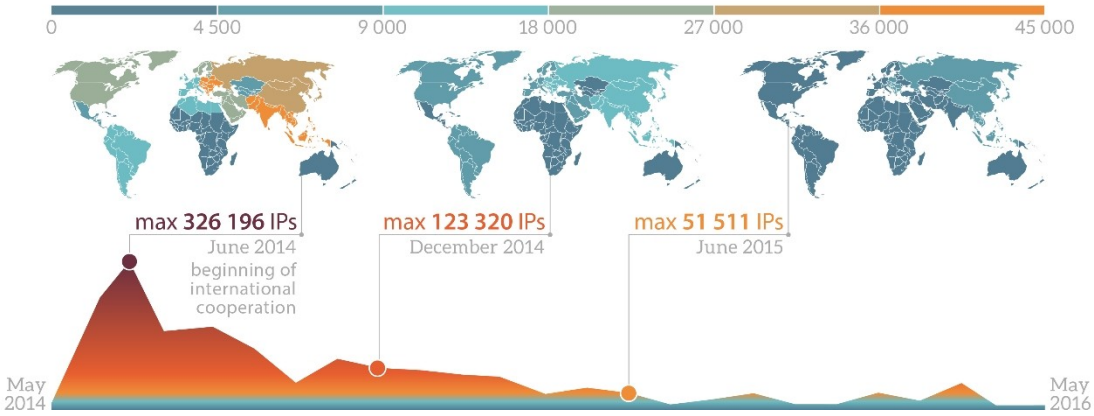
Several studies demonstrate that the vulnerability to digital risks and total costs it im can be reduced, provided certain features are in place, including a national cybersecu strategy or an adequate institutional framework. Both the EU and the US cybersecurit strategies list stronger relations with international partners as one of the mechanisms towards preserving open, free and secure cyberspace. They also recognise engageme with key partners as a way towards promoting their respective political, economic and strategic interests. Given the scope of their bilateral relationship, shared values and t exposure to similar threats, the EU and the US are natural partners in cooperat countering online criminal networks, improving resilience of their societies, and countering the threat posed by third parties.

Fight against criminal networks online

The need for transatlantic cooperation and the convergence of interests is clearly visi in the case of the fight against cyber crime. In April 2016, an international cyber gang unleashed a malware known as GozNym that has stolen US$4 million from more than 24 American and Canadian banks, credit unions and popular e-commerce platforms in just a few days. A week after launching the attack campaign in North America, GozNy operators spread a new European configuration that attacked corporate, investm banking and consumer accounts held with major banks in Poland and Portugal. SWIFT, the global financial network used by banks to transfer billions of dollars every day, wa also a victim of cyber-attacks in which the perpetrators had altered SWIFT software a used the system to send fraudulent messages – a process that cost the Banglad Central Bank account at the New York Federal Reserve Bank a total of US$81 million.

Against this background, EU-US law enforcement cooperation in the fight against cybercrime is addressed in the **EU-US Working Group on Cybercrime**. Specific commitments in this domain – many of which require cooperation over years - w made at the EU-US Justice and Home Affairs ministerial meeting in Riga in June 2015, include: facilitating law enforcement exchanges, including but not limited to th pertinent to child sexual abuse offences, travelling child sexual offenders and networ intrusion; collaboration in fighting and disrupting cybercrimes; and enhancing cybersecurity including through joint research; and promoting adoption of the Budape Convention and training practitioners on its provisions. In addition, representatives fr counterpart US agencies have been placed within Europol's Cybercrime Centre (EC3) Eurojust with the aim of supporting operational cooperation. For instance, in April 201 a multinational law enforcement operation led by the EC3 and the Joint Cyberc Action Taskforce (J-CAT) disrupted the operations of the Beebone botnet, that had installed malware on about 12 000 computers in around 195 countries. Cooper between Europol, law enforcement cybercrime units in Member States and technolog industry partners operating across the Atlantic helped to dismantle botnet, know Zeroaccess, which was responsible for infecting over 2 million computers worldwide a had cost online advertisers US$2.7 million each month. Cooperation between law enforcement agencies from across the world, led by the FBI and supported by the EC Europol, also ensured the disruption of the Gameover Zeus botnet and the seizure o computer servers crucial to the malicious software known as CryptoLocker (Figure 5).

Figure 5 - Number of IP addresses infected with Gameover Zeus botnet over time



Data source: CyberGreen, 2016.

Improving resilience of networks

Beyond the fight against cybercrime, the EU and US have a strong interest in develop joint approaches – or at least ensuring a close coordination and sharing best practices with regard to protection and building resilience of their critical infrastructure network (e.g. energy, transportation, financial systems). Given the extent to which the EU and are interconnected, the economic and social implications of such attacks on either sid of the Atlantic could have a huge impact on the economy, and potentially stability, ac the transatlantic area. For instance, the US Industrial Control Systems Cyber Emergen Response Team (ICS-CERT) found that a synchronised and coordinated cyber-attack, s as the one carried out on a section of the Ukrainian power grid in December 2015, co cost anything between US$243 billion and US$1 trillion dollars. Attacks on critical infrastructure – albeit on a smaller scale – are nevertheless quite common. In 2015, a report released by the German Federal Office for Information Security confirmed that German steel mill suffered 'massive' damage as a result of a cyber-attack manipulati and disrupting control systems to such a degree that a blast furnace could not be pro shut down. In April 2016, multiple forms of malware were found in a German nuclear energy plant in Gundremmingen. Even though the types of malware discovered sugg an accidental infection rather than a targeted attack, the news reaffirmed a persisten vulnerability of critical infrastructure networks.

Given that there is almost universal agreement on the growing risk of cyber-attacks o critical infrastructure, the EU and US need to enhance their cooperation in preparing f a transatlantic 'cyber Katrina'. Currently, the **EU-US Working Group on Cybersecurity** provides a setting for discussions along several strands, including those focused on p private partnerships and incident management, but it is clear that this dialogue woul benefit from an additional political impetus. As part of the effort to improve the resilie of their networks, over 60 participants from 16 EU Member States and the US contrib to the first joint EU-US cyber exercise, 'Cyber Atlantic 2011' facilitated by the Europea Network and Information Security Agency (ENISA) and Department of Homeland Secu (DHS). The objectives of the exercise included improving cyber-crisis managem cooperation, identifying the procedures and mechanisms employed during a cyber-cri and exchanging good practices on approaches to international cooperation. Since 201 EU Member States and the US have participated in the NATO cyber defence exercises 'Locked Shields'.

Countering threats to national security

Due to the fact that criminal networks often operate in several jurisdictions, or receiv
support from third country governments, and that some cyber-attacks might pose a
serious threat to a state's security – potentially resulting in a military conflict –
transatlantic discussion about secure and safe cyberspace necessarily involves bo
diplomats and military staff. Several instances illustrate that this is indeed the case. F
example, in November 2015 air traffic control systems across much of Sweden
unavailable, resulting in the cancellation of multiple domestic and international flights
the airports of Arlanda, Landvetter and Bromma. Sweden reportedly suspected that a
hacker group linked to Russian military intelligence service (GRU) was responsible for
attack and passed this information on to NATO members in neighbouring countries su
as Norway and Denmark. Another example is a growing cyber threat posed by terroris
groups. Even though to date the attacks by jihadi groups such as ISIL/Da'esh have be
limited to compromising social media accounts or defacing websites, the announcem
of a new group called the 'United Cyber Caliphate' (following the formal merger of se
groups) raises new concerns regarding ISIL/Da'esh's cyber capabilities. In both cases,
need to think in broad national security terms (something which law enforcement and
critical infrastructure operators are not always used to doing), and a possible respons
going beyond law enforcement, technical measures or national borders (which
actors are not empowered to do), brings diplomats and 'cyber soldiers' into the pictur

With regard to international security, the EU and US seek greater stability and promot
norms of responsible state behaviour in cyberspace. The basis for EU-US cooperation
this respect is provided in the report by the **United Nations Governmental G
Experts** (UN GGE), published in June 2015, to which both sides have actively contribu
The report sets out the norms regulating state behaviour. These forbid states
knowingly allow their territory to be used for cyberattacks; to conduct or know
support attacks that damage critical infrastructure; to conduct or knowingly su
activity intended to harm the information systems of another state's emergency resp
teams (CERT/CSIRTS), and to use their own teams for malicious international activity.
efforts aimed at promoting the implementation of these norms globally and th
regional organisations (e.g. **OSCE, ASEAN Regional Forum, Organization of Ame
States**) offer a possibility to streamline EU-US cooperation in this respect. The
Statement adopted in 2015 is seen as a significant step towards achieving globa
agreement on some of these norms. However, their voluntary nature means that furt
diplomatic efforts are likely to be needed in order to find a consensus with countries l
China and Russia on the practical steps towards their implementation. The EU and US
also at the forefront of the discussion about confidence-building measures that would
minimise the risk of misunderstandings and help avoid escalation and conflict in
cyberspace. To that effect, both sides work closely in the framework of the Organisati
for Security Cooperation in Europe (OSCE). The agreement between the **EU Computer
Emergency Response Team (CERT-EU)** and the **NATO Cyber Incident Response
(NCIRC)**, signed in February 2016, provides an additional opportunity to streng
cooperation between the EU and the US, but the details of its implementation still ne
to be worked out.

Looking ahead: Potential projects and challenges

As some of the high level attacks in 2015 have demonstrated, the growing digital risk
the transatlantic economy and security provide strong incentives for closer EU-
cooperation on enhancing cybersecurity and fighting cybercrime. In addition, with

increasing regulatory and legislative activity in the field of cybersecurity, absen cooperation between legislators on both sides of the Atlantic could have a sign negative impact – and a potential cost – as it is likely to lead to divergent regulations standards, including on encryption or data protection. At transatlantic level, a wide spectrum of cyber-related issues is pursued **through the EU-US Cyber Dialogue** established in the aftermath of the EU-US Summit in 2010. Several meetings of the Dialogue to date have confirmed the close alignment on many issues, including cybercrime, building resilience, countering threats posed by third parties, eradicating havens in cyberspace, and protection of human rights online and offline.

While the European and American interests in this policy area are to a large overlapping – with several initiatives already underway – there is a clear need for a 'r map' that would provide the ongoing efforts with more structure and dynamism. Th following functional blocks of cooperation, to be pursued by all groups of actors involv could provide the framework for future initiatives and projects across the various poli areas (for a detailed description of actors and actions by policy area, see the Annex).

- *Improved information sharing and situation awareness* through joint identificat and/or exchange of best practices – including on cooperation with private sector an other stakeholders; joint threat analysis and exchange of information about t vectors and possible mitigation techniques; regular discussions about planned legislation or legislation in progress; regular exchanges aimed at identificatio opportunities/'low-hanging fruits' and potential obstacles to cooperation.
- *Strengthening joint response capacities and operational cooperation* by promoting better understanding of the emerging Critical Information Infrastructure lands (e.g. smart grids, botnets, cloud computing); developing good practices (e.g. approaches to data breach notifications), and joint exercises. This implies a cooperation with the private sector, which is often the owner of the infrastructure c the critical information, and whose approach and interests are not always aligned w those of the government (e.g. the ongoing debate about encryption and backdoors At the international level, such projects could focus on building capacities in countries, in particular through the promotion of adequate legal frameworks compliant with the provisions of the Council of Europe Convention on Cybercrime), setting up institutions (e.g. Computer Emergency Response Teams), and crea policy frameworks (e.g. national cybersecurity strategies).
- *Improving across-the-board awareness of digital threats and vulnerabilities* through joint awareness-raising campaigns (such as the existing Cyber Security Aware Month,'Stop.Think.Connect') as well as political and institutional dialogues. In th sense, the role of the existing venues, such as the Transatlantic Business Dialogue (TABD), Transatlantic Consumers' Dialogue (TACD) and Transatlantic Policy Network (TPN), could be re-assessed.
- *Building trust and confidence – both in the digital environment and with regard to s behaviour* – through more transparency providing space for genuine multi-stakehol consultation processes involving governments, private sector and civil society; developing a common vocabulary related to cybersecurity in order to avoid the risk misunderstanding and misperceptions in the field of cyber insurance policies), and joint exercises which allow for a better understanding of commonalities differences. At the international level this would imply promoting (through worksho seminars, joint research projects) confidence-building measures and norms of

responsible behaviour in cyberspace, based on the measures proposed by the OSC and the UN GGE 2015 report.

Despite substantial evidence that closer EU-US cooperation in the field of cybersecuri and the fight against cybercrime is a necessity, one cannot ignore the simple fact tha two sides of the Atlantic are also competitors on global markets. Consequently, there a substantial risk that transatlantic cooperation in this policy area becomes tra between calls for digital protectionism in Europe and a conviction of digital supremac the United States. For instance, President Barack Obama described the EU's position data protection in the US as intended to 'carve out their [the EU's] commercial intere faced with the EU's own incapacity to compete with US-based companies. Sen Wyden (D-OR) called the Court of Justice ruling in the Safe Harbour case 'open season on American businesses. The European Union's dependence on third parties' software and hardware (see Figure 4) has led some countries to a belief that Europe urgently n to develop its own 'digital strategic autonomy', characterised notably by the development of a European digital security industry, while encouraging design production in Europe, and the encouragement of the emergence of a robust European certification framework to generate internationally competitive European digital champions. In an effort to protect European digital space, there are also voices calling the development of an alternative approach to the global 'free flow of data' which wo support the ability of the EU and Member States to locate in Europe data requirin certain level of protection, as well as promote the EU's vision of digital security and v in international negotiations on cyberspace. The latter point might be particula problematic given the tendency in the United States, but also in some Member States overly securitise the digital space.

Annex - Building blocks for cooperation and possible projects

	POLICY AREAS			
	Cybercrime	Cybersecurity	Cyber diplomacy	Cyber defence
Points of convergence				
Approach	Cybercrime poses a significant threat to citizens' prosperity and undermines the potential for human development. As such, it requires across the board involvement from government, the private sector, and civil society.	Our reliance on internet-based platforms for delivery of services increases as does the vulnerability of critical infrastructure networks. Improving resilience of networks is therefore a key priority for multi-stakeholder cooperation.	An international system is as strong as its weakest link and therefore capacity building in third countries plays an important role. Norms of behaviour and confidence building measures are key to preventing cyber conflicts.	The protection of military installations and sectors critical for a nation's functioning is a matter of national security.
Primary actors	Law enforcement, private sector (service providers, tech companies)	Private sector (operators, service providers), CERTs	Diplomats, development agencies	Diplomats, military, intelligence services
Main framework for cooperation	EU-US Working-Group on cybercrime	EU-US Working-Group on cybersecurity	EU-US cyber dialogue	EU-US cyber dialogue NATO
Functional blocks and possible concrete projects and actions				
Institutional	• Establishing a high-level EU-US Digital Council aimed at breaking bureaucratic silos and connecting dots between broad policy objectives; • Strengthening and streamlining dialogues; • Bolster efforts to increase the understanding of cyber-related issues among legislative, executive and judicial branches.			
Regulatory cooperation	Improve the effectiveness of Mutual Legal Assistance Treaties	Including cyber resilience as a cross-cutting issue in all transatlantic dialogues	Consider advantages and disadvantages of establishing a 'cyber sanctions' regime	Continue cooperation on developing cyber norms under the threshold of armed conflict
	Continued support for the Global Alliance against Child Abuse Online	Consider introducing 'cyber maturity adequacy finding' in international agreements, including through developing common standards	Ensure full respect for and protection of human rights online	
Operational cooperation	Increase the capacities of law enforcement agencies to conduct joint operations	Define minimum common digital security and privacy requirements across different sectors	Adopt common positions or statements following major cyber accidents that might suggest third countries involvement	Joint exercises: NATO cyber defence exercises 'Locked Shields' involve both the US and the EU but it is not the case for EU run exercises.
		Joint impact assessments for proposed regulation and standards		

	POLICY AREAS			
	Cybercrime	**Cybersecurity**	**Cyber diplomacy**	**Cyber defence**
Joint-response capabilities	Exchange training practices, including through establishing 'Erasmus' for cyber experts	Expanding the mandate and resources of ENISA to strengthen its international cooperation capacities	Seek greater stability in cyberspace within the UN and regional organisations	Exchange of best practices on partnership with industry, including EU, US but also NATO Industry Cyber Partnership (NICP)
		Establish a 'phone book' with points of contact at all levels and sectors	Promote non-governmental venues for cybersecurity, e.g. Meridian Process, Global Forum on Cyber Expertise	
		Conducting stress tests across different areas of Critical Infrastructure Protection		
Information sharing	Exchange information on emerging trends and needs in view of evolving cybercrime and cybersecurity patterns	Exchange best practices on cooperation models with private-sector and service providers	Compare modalities of responding to coercive cyber operations	Enhanced cyber defence information sharing to improve prevention, prediction, detection and response (interoperable information sharing operational standards) within EU-NATO agreement but also with EU Military Staff (EUMS)
		Establish a working group that would prepare an 'inventory' of possible joint actions	Compare notes from different dialogues and engagements with third countries	Share cyber defence best practices on technical innovations, incident handling methodologies and secure configuration of networks.
Situational awareness	Joint threat analysis between EC3 and FBI	Joint threat assessment ENISA, CERT-EU and CERT-US		Development of a joint vocabulary
		Developing a better understanding of the emerging Critical Information (CII) landscape (e.g. smart grids, botnets, cloud computing)		Share information about indicators of compromise, situational awareness, reports, bulletin and information on techniques, tactics, and relevant mitigation measures.
Awareness-raising	Joint campaigns	Joint campaigns		
Trust and confidence	Transparency	Exercises	Promote confidence building measures in cyberspace	Visits to facilities and laboratories and contractor facilities
				Exchange information about information management practice

Main references

Carl Bildt and William E. Kennard, Building a Transatlantic Digital Marketplace: Twenty steps toward 2020, Task Force on Advancing a Transatlantic Digital Agenda, Atlantic Council, April 2

Center for Strategic and International Studies, Net Losses: estimating the global cost of cybercrime, June 2014.

Melissa Hathaway, Cyber Readiness Index 2.0, Potomac Institute for Policy Studies, Novembe 2015.

Patryk Pawlak (ed.), Riding the digital wave. The impact of cyber capacity building or development, Report 21, EU Institute for Security Studies, December 2014.

The World Bank, Digital dividends, World Development Report, 2016.

Disclaimer and Copyright

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