Analysis

"Tackling new threats upon which the security and prosperity of our free societies increasingly depend": the EU-US Working Group on Cyber Security and Cyber crime

Chris Jones

A trans-Atlantic working group has been created to share best practices, exchange information, and look at specific issues such as cyber incident management and child pornography. The group's activities promote increased internet regulation and the development of military capabilities for cyberspace, which invariably come at the expense of individual rights and freedoms.

The last year has seen significant developments in both national and European policies that attempt to address the issue of cyber security and cyber crime. One particularly significant move has been the establishment, following the November 2010 annual EU-US Summit, of a new transatlantic Working Group on Cyber Security and Cyber Crime. The statement announcing the group's formation noted the intention of the EU and US to "address a number of specific priority issues" - cyber incident management, public-private partnerships, awareness-raising, and cyber crime - and "report progress within a year".

While cyber crime covers issues such as fraud, the theft and misuse of personal data, phishing, the illicit distribution and sharing of copyrighted content, and other related issues, cyber security is a broader term. The EU apparently lacks its own definition of cyber security, although the European Organisation for Security ("the leading European organisation for the private security sector providers of technology solutions and services"0 [1]) defines it as:

> *The need to prevent from, prepare for, detect, respond to and recover from any hazard or illicit content in the cyberspace, covering networked infrastructures, including [the] Internet. [2]*

The definition used by the US Department of Homeland Security is a little more thorough:

> *[Cyber security is] the prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability. Includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. [3]*

Policies aimed at ensuring cyber security are therefore aimed not just at the information transmitted via digital networks, but also at the physical infrastructure facilitating that transmission. Network infrastructure such as servers and databanks permit the functioning of, for example, water and electricity supply systems.

The drive towards greater cyber security has led to a profusion of institutions, bodies, resolutions, statements, action plans, policies and legislation in the last decade or so. A number of EU measures have been geared towards cyber security, with a notable increase in the last year.

While there is undoubtedly a need to prevent malicious activity directed towards networked infrastructure, cyber security policy requires a balance between the powers of the state and the rights of individuals. Policies ostensibly aimed at 'securing' cyber space can have detrimental effects on individual rights, at the same time as opening new areas in which the state and other actors can exercise coercive power. This is illustrated most vividly by the ongoing debates surrounding intellectual property enforcement (for example, with the UK's Digital Economy Act), by which internet service providers would be obliged to adopt a police function in determining whether websites and internet users have broken the law.

Following an outline of the ideas, structure and working method of the EU-US Working Group (hereafter the WG), the four "priority issues" will be examined in the context of a "Concept Paper" (CP) that was issued in April 2011 for the Transatlantic Cyber Security Research Workshop held at the Hungarian Embassy in the United States. [4] This will be used to illustrate some of the potential issues that arise when states invoke the need for greater cyber security, and, more specifically, some of the more problematic approaches taken by the United States, the EU, and the EU's Member States.

Structure and composition of the Working Group

The EU-US Working Group is composed of four 'Expert Sub-Groups' (ESG), in which most activities are conducted. The WG's main role is to "[take] stock of the progress of the ESG. It meets in ad hoc formats to manage activity at a senior level. It may also, "as appropriate, [get] the necessary political steering and guidance on the political level."

The four ESG deal with the "specific priority issues" noted above. Groups 1, 2 and 3 deal with cyber security-related issues (cyber incident management, public-private partnerships, and awareness-raising respectively), and are chaired by the same two individuals: Andrea Servida from the EU Directorate General on the Information Society and Media (DG INFSO) and an unnamed "US counterpart." ESG 4 (cyber crime) is co-chaired by Jakub Boratynski for the EU (head of the Commission's Directorate-General for Home Affairs' 'Fight against organised Crime' unit) and B. Shave for the US.

A number of heavyweight EU and US institutions are represented in the makeup of the ESG. EU representation will come from relevant Directorates-General (such as INFSO and HOME); the European External Action Service (EEAS); the Presidency of the Council; the Counter Terrorism Coordinator; the EU representation office to the US; EU agencies such as European Network and Information Security Agency (ENISA), Europol and Eurojust; and "experts from the EU Member States' competent national authorities". For the US, participants will come from the Department of Homeland Security (DHS); the US Secret Service (USSS); the Immigration and Customs Enforcement (ICE); the Department of Commerce (DoC); the National Telecommunications and Information

Administration (NTIA); the National Institute of Standards and Technology (NIST); the Department of State (DoS); the White House and National Security Council (NSC); the Department of Justice (DoJ); and the Federal Bureau of Investigation (FBI). Furthermore, experts "selected on an ad hoc basis" may also be invited to participate.

Guidance to the Working Group itself will come, on the US side, from the Secretary of State; the Attorney General; the Secretary of Homeland Security; and the Special Assistant to the President and Cyber security Coordinator. For the EU, guidance will stem from the European Commission Vice-President for the Digital Agenda; the Commissioner for Home Affairs; the Presidency of the Council; the High Representative of the Union for Foreign Affairs and Security Policy; the office of the President of the European Council; and the office of the President of the European Commission.

Accountability and Activities

Any work undertaken by the Working Group or the Expert Sub Groups is subject to senior authority:

> *All configurations (WG, ESG) get their political guidance and high-level decisions formally approved from their respective political authorities, who shall in parallel maintain their EU-US bilateral contacts as appropriate.*

Given the number of different state agencies from both the EU and US involved in the WG, it seems that there is a keen interest from both parties in the potential benefits of cooperation. It is also alarming (but perhaps not surprising) that there is so little information available on the undertakings of the WG. So far there seem to have been two formal meetings of the group: the first on the 24th and 25th February 2011 on Internet governance; the second on 28th and 29th June 2011 on child pornography.

A number of questions submitted to the European Commission by Marietje Schaake MEP in May 2011 attempted to establish the necessity and aims of the WG. [5] An attempt was also made to ascertain information on the forthcoming EU cyber crime centre, the European information-sharing and alert system and the recently-established Computer Emergency Response Teams (CERTs). Nine separate questions covered topics such as the need for new institutions; means of monitoring data flows; the types of crime to be targeted; information-sharing between the EU and US; commercial relations; fundamental rights and democratic oversight.

The answer from Cecilia Malmström on behalf of the Commission was a paltry three short paragraphs. In response to Ms Schaake's question regarding public information on the WG, Ms Malmström noted that "the Commission does not share the Honourable Member's view that little information about [the WG] can be found", and mentioned three press releases – hardly a useful source of detailed information. The second paragraph merely restated, in briefer form, the official aims of the WG, which can itself be found in the press releases. The third and final paragraph rejected the notion that vested commercial interests have overplayed the threat from cyber crime, and suggested that the WG "is a timely and strategically highly significant response" to assessments from Europol, Interpol, and industry.

Issues identified by the Working Group

According to the Concept Paper, the WG was established in order to "tackle new threats to the global networks upon which the security and prosperity of our free societies increasingly depend".

The increasing reliance of everyday life upon digital networks has led to an increasing recognition in recent years of the need to make those networks more secure, with a growing number of states developing their own cyber security strategies. The UK's Cabinet Office notes that society is "now almost completely dependent on cyber space," [6] therefore requiring robust efforts to deal with cyber crime and enhance security. Quite what this will mean in practice will become clearer as states develop and implement policies, although recent and current practice provides some indication.

Perhaps one of the most significant issues relates to the military use of cyber space. It is clear that the cyber security policies developed by states are far from being simply 'defensive'. The Pentagon has stated that "it is boosting efforts to build offensive cyber arms for possible keyboard-launched US military attacks", [7] with subsequent statements announcing that the "US military is now legally in the clear to launch offensive operations in cyberspace". [8] Such a statement may raise questions about the legality of previous computer network attacks by the US, as during the invasion of Iraq. [9] The UK is also working on the development of "an offensive capability to deal with cyber threats". [10] These developments cannot be considered just obvious extensions of traditional military practice. The increasing propensity of state and non-state actors to utilise digital networks in offensive military strategy blurs "traditional binaries of war and peace, the local and the global, the civil sphere and the military sphere, the inside and the outside of nation-states." [11]

As of yet, there is no indication that the EU and the US are cooperating on the development of offensive strategies. At least publicly, joint action geared towards dealing with cyber-attacks on critical infrastructure has been resolutely defensive. Nevertheless, the establishment of the WG certainly provides a forum in which such issues can be discussed.

Cyber Incident Management

The first of the four issues concerning the WG is Cyber Incident Management. The scope of activities to be organised under this heading includes the development of "broad scenarios", the sharing of "good practices for promoting the resilience and stability of networks", and the exchange of good practice on "how to work and cooperate across sectors; engage with other countries; exchange information between Governments". The expected outcomes include a series of joint workshops in anticipation of joint cyber exercises, and an "alignment plan for developing country capacity-building on cyber security incident management". Expert Sub-Group 1 deals with these issues, and it is here that the more militaristic element of cyber security has been expressed. This is demonstrated by the first joint exercise undertaken by the two parties: "Cyber Atlantic 2011".

With the CP outlining the need for "a joint cyber exercise in the timeframe 2012-2013", Cyber Atlantic arrived somewhat ahead of schedule in November 2011. It was clearly an extensive project, with "security experts" from the US, the EU, and more than 20 EU Member States given the job of dealing with:

> *Simulated crises affecting national security. In the first scenario, a targeted attack burrowed into the network of an EU country and stole sensitive data there. In the second, an industrial control system used to manage machinery in a power plant was attacked, in an attempt to disrupt its operations. [12]*

The emphasis here is clearly on defensive capabilities. However, it would not be presumptuous to assume that offensive capabilities have at least been considered by the WG. As noted above, both the US and UK have recently publicly announced offensive cyber-warfare programmes. Germany too

has “declared war on hackers” with a new Cyber Defence Centre, the job of which is to “spot and evaluate attacks, and to develop counter strategies”. [13] The US Congressional Research Service as far back as 2001 listed the UK, France, Germany, Russia and China as states that are “incorporating cyberwarfare as a new part of their military doctrine”. [14] One writer asserts that there are “more than 100 nation states that have set up military and intelligence cyberwarfare units”. [15]

Whether the EU will be able to muscle in on Member States’ cyber-warfare policies is questionable – most Member States remain strongly nationalistic when it comes to defence issues. A number of EU Member States – including the Czech Republic, France, Germany, the Netherlands and the UK – have, in the last year, launched their own national cyber security strategies. The EU has yet to adopt its own, but it has a number of institutions and policies geared towards, amongst other things, supporting those Member States that wish to develop their own policies and initiatives on cyber security.

The ‘Trio’ (the current Polish and future Danish and Cypriot Presidencies of the Council) have also made cyber security a priority, in light of “cyber attacks against the Commission and the EEAS in March 2011”. A document from July 2011 states that the Trio will “explore possibilities to develop global and regional responses to the threats linked to cyber crime and to develop strategies on cyber security”. [16] Any such work is likely to build on a Communication issued by the Commission in March 2011 on “Critical Information Infrastructure Protection – ‘Achievements and next steps: towards global-security’.” This document notes that there is a “trend towards using ICT [Information and Communication Technologies] for political, economic and military predominance, including through offensive capabilities.” [17]

New institutions at EU level include:

- The Computer Emergency Response Team (CERT, a unit pulling together "existing IT security departments from the Commission, the Parliament and the Council to handle cyber attacks on all EU institutions"); [18]

- The European Network and Information Security Agency (ENISA, "Securing Europe's Information Society"); [19]

- A soon to be established "EU cyber crime centre", with which Europol is apparently keen to be involved. [20]

Related work is undertaken by the European Forum for Member States (“established to foster discussions and exchanges between relevant public authorities regarding good policy practices, with the aim of sharing policy objectives and priorities on the security and resilience of ICT infrastructures” [21]) and the European Public-Private Partnership for Resilience (EP3R), [22] itself established “within the framework of the initiative on Critical Information Infrastructure Protection”, abbreviated to CIIP. [23] All three come under the remit of the Directorate-General for the Information Society, DG INFSO. Europol also has its own Cyber crime Task Force.

ENISA is currently the subject of a proposed Regulation of the European Parliament and Council that would “strengthen and modernise” the agency. Without mandating any operational tasks, the Commission has proposed that “ENISA should act as an interface between cyber security experts and public authorities involved in the fight against cyber crime”. A “gradual increase” in “financial and human resources” will allow this. [24] The European Data Protection Supervisor has noted a number

of problems with the proposed new tasks for ENISA including lack of clarity, legal uncertainty, and potential function creep amongst others. [25] A Parliament vote on the proposed Regulation is currently due in early 2012.

It is not only state and governmental institutions that are concerned with cyber security. The private sector also has enormous commercial interests in the use of digital networks. Any attempt by governments to protect digital networks from perceived "threats" must involve the private sector, as the majority of the infrastructure and equipment permitting the continued operation of such networks is in private hands.

Public Private Partnerships (PPP)

The Concept Paper makes clear that the WG is also expected to enable the development of "compatible approaches" to Public Private Partnerships (PPP), based on:

> *(a) key assets, resources and functions needed to ensure the continuity of electronic communications services;*
>
> *(b) good practises (including baseline requirements, if appropriate) for the security and resilience of vital ICT infrastructures based on risk management;*
>
> *(c) shared coordination and cooperation mechanisms to prevent, mitigate and react to cyber-disruptions and cyber-attacks.*

The mention in point (c) of the need to be able to react is a hint that offensive capabilities have not been side-lined by the WG. However, the section on PPP is broadly devoted to other issues.

It is expected that the group will produce reports on topics of mutual interest "including best practices and models to engage with the private sector"; national programmes for dealing with botnets; good practices on cyber security in the private sector; legislative development; an action plan intended to draw the private sector into "cooperative activities with governments, on selected areas"; and a set of "common principles and guidelines on the resilience and stability of the Internet as well as reliable access to it".

The questions submitted by Ms Schaake to the European Commission (noted earlier) on the issue of the WG asserted that the risks posed by cyber security and cyber crime required more analysis before the establishment of legislation and policy – "it is necessary to know facts and figures instead of basing policy on perceived risks" that have been asserted by "business interests." This may well be true. Nevertheless, "the cyber security market is witnessing an unprecedented growth in the next decade". [26] Many businesses will therefore likely be pleased with the WG's statement that:

> *While PPP represents a specific priority area, it also cuts across all other priority areas, and thus may be included in work in those areas as well.*

The UK's Cabinet Office commissioned a study on the cost of cyber crime to the UK economy, which was estimated by the study's authors to be in the realm of £27 billion. This figure has been dismissed as "meaningless" by Tyler Moore of the University of Cambridge, due to failings in its methodology and calculations. [27]

There is no indication that the WG has so far encouraged the formation of any particular public private partnership, although according to the CP, an analysis of good practice, initiatives, and models for national PPPs should have been completed in summer 2011.

Awareness-raising and cyber crime

As regards awareness-raising, the Working Group will seek to share best practice and exchange information:

> *In particular on how best to involve [ISPs] and technology providers in the delivery of messages to users about online behaviour and in the development of awareness raising materials.*

The first major crime issues for the WG is child pornography, for which a roadmap will be developed seeking to identify more effective ways to take down websites containing illegal content, as well as investigating effective channels for prosecution. There is also the technologically ambitious goal of examining "technological solutions to detect previously identified CP images from all locations on the internet". By June this had become more specific, with the US proposing to use “photo DNA software made by Microsoft and available for free for detecting and deleting child pornography pictures on internet”. The EU was apparently “interested in the proposal.” [28]

The Working Group will also develop a programme aimed at "eliminating illegal use of Internet resources, such as IP addresses and DNS (domain names)." Part of this process involves an attempt to have the Governmental Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN) endorse "law enforcement recommendations", as well as to "collaborate, directly and through the GAC, with ICANN on [a] roadmap for [the] implementation of law enforcement recommendations".

ICANN is a “not-for-profit public-benefit corporation with participants from all over the world dedicated to keeping the internet secure, stable and interoperable.” Its essential purpose is to ensure that the unique identifying numbers underlying internet addresses are globally coordinated. As the organisation’s website goes on to note, it:

> *Doesn’t control content on the internet. It cannot stop spam and it doesn’t deal with access to the internet. But through its coordination of the internet’s naming system, it does have an important impact on the expansion and evolution of the internet. [29]*

In May 2011, a bilateral meeting between the EU and US authorities announced that “reforms [to ICANN] are necessary” in order to:

> *[R]einforce the transparency and accountability of the internal corporate governance of ICANN, to enhance ICANN’s responsiveness to governments raising public policy concerns in the GAC and to improve the way decisions affecting country-code Top Level Domains are made. [30]*

The Concept Paper also notes that the EU and US are seeking the implementation by ICANN of law enforcement recommendations, which includes the “implementation by DNS registrars and registries of Top Level Domain names”. The specifics of these law enforcement recommendations remain unknown. Similarly cryptic is the statement that there will be coordination to ensure “IP addresses are allocated, assigned and recorded in the most secure and stable manner”.

There are two final aspects of awareness raising to be undertaken by the EU-US Working Group. Firstly, attempts will be made to increase the number of states party to the Council of Europe Convention on Cyber crime. In a July 2011 meeting of EU-US JHA Senior Officials, the US "called again for full ratification by the remaining 9 EU Member States of the [convention]." Consideration will also be given to the possibility of taking joint approaches in international forums, such as the expert group on cyber crime of the UN Office on Drugs and Crime. On this issue, the minutes of the July 2011 meeting state that "the EU and the US should work together in the UN to avoid dilution" of the body of international law on cyber crime. [31]

Conclusions

The Concept Paper outlines a substantial base on which cooperation between the EU and US can proceed on the issues of cyber crime and cyber security. One year from the establishment of the Working Group, the EU and US met again for their annual official summit. Despite what the statement goes on to say, it is not necessarily the case that "respect for fundamental freedoms online, and joint efforts to strengthen security, are mutually reinforcing". Moves towards tighter regulation and even outright censorship of the internet and the development of military capabilities for cyberspace may strengthen the security of states and their corporate allies, but they potentially do so at the expense of individual rights and freedoms. If the work of the WG continues in its current, secretive fashion, then greater scrutiny and more pressing questions must accompany it.

Endnotes

1.European Organisation for Security, 'What is EOS?':

http://www.eos-eu.com/AboutEOS/WhatisEOS/tabid/55/Default.aspx

2. European Organisation for Security, 'Towards a concerted EU approach to cyber security', September 2010, p.8

3. Department of Homeland Security, National Infrastructure Protection Plan, 2009, p.109,

http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

4. Transatlantic Cybersecurity Research Workshop at the Hungarian Embassy under the Presidency of the Council of the European Union, 22nd April 2011,

http://www.huembwas.org/News_Events/20110408_cyber_conf/summary_elemei/MD-018a-11-EU%20US%20WG%20-%20Concept%20paper%20-%20CL%20201110413_US.pdf

5. Marietje Schaake, Question for written answer to the Commission (E-004816/2011), 17th May 2011,

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+WQ+E-2011-004816+0+DOC+XML+V0//EN&language=BG

6. Cabinet Office, 'The cost of cyber crime',

http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

7. Jim Wolf, 'U.S. says will boost its cyber arsenal', Reuters, 7th November 2011

http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107

8. Brid-Aine Parnell, ‘US general: ‘We’re cleared to cyber-bomb enemy hackers’, The Reigster, 17th November 2011,

http://www.theregister.co.uk/2011/11/17/us_military_cyberspace/

9. Stephen Graham, ‘Cities Under Siege’, 2010. London: Verso, p.291

10. Duncan Gardham, ‘Britain prepares cyber attacks on rogue states’, The Telegraph, 26th November 2011,

http://www.telegraph.co.uk/news/uknews/defence/8916960/Britain-prepares-cyber-attacks-on-rogue-states.html

11. Stephen Graham, ‘Cities Under Siege’, 2010. London: Verso, p.294

12. Dan Goodin, 'US, Europe throw their very first joint cyber-war party', The Register, 4th November 2011

13. Matthias von Hein, ‘Germany declares war on hackers with new cyber defence centre’, Deutsche Welle, 1st April 2011:

http://www.dw-world.de/dw/article/0,,14960339,00.html

14. Congressional Research Service, ‘Cyberwarfare’, 19th June 2001, p.2,

http://www.fas.org/irp/crs/RL30735.pdf

15. Peter W. Singer & Noah Schachtman, ‘The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity is Misplaced and Counterproductive’, 15th August 2011, Brookings,

http://www.brookings.edu/articles/2011/0815_cybersecurity_singer_shachtman.aspx

16. Note from: Polish, Danish and Cyprus Presidencies to: Delegations, ‘JHA External Relations – Trio Programme’, 4th July 2011, p.6 (EU doc. no. 12004/11),

http://register.consilium.europa.eu/pdf/en/11/st12/st12004.en11.pdf

17. Commission Communication, ‘Critical Information Infrastructure Protection - ‘Achievements and next steps: towards global-cyber security’’, 31st March 2011, COM(2011) 163 final

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0163:FIN:EN:PDF

18. Valentina Pop, 'EU institutions to create new cyber defence unit', EU Observer, 20th May 2011

19. European Network and Information Security Agency,

http://www.enisa.europa.eu

20. Valentina Pop, 'Europol wants to host EU cyber crime centre', EU Observer, 14th November 2011

21. CIIP – Implementation activities – Pillar 1,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/pillar_1/index_en.htm

22. European Public-Private Partnership for resilience – EP3R,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/ep3r/index_en.htm

23. Critical Information Infrastructure Protection,

http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm

24. Progress Report from: Presidency to: Council, 'Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)', 19th May 2011, p.1-2 (EU doc. no. 10296/11),

http://register.consilium.europa.eu/pdf/en/11/st10/st10296.en11.pdf

25. European Data Protection Supervisor, Opinion on the proposal for a Regulation concerning the European Network and Information Security Agency (ENISA), 1st April 2011, p.2:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:101:0020:0024:EN:PDF

26. Frost & Sullivan, 'Cyber Security – From Luxury to Necessity', February 2011, p.6,

http://www.frost.com/prod/servlet/cio/225170443

27. Tyler Moore, 'Why the Cabinet Office's £27bn cyber crime cost estimate is meaningless', Light Blue Touchpaper, 17 February 2011,

http://www.lightbluetouchpaper.org/2011/02/17/why-the-cabinet-offices-27bn-cyber-crime-cost-estimate-is-meaningless/

28. General Secretariat of the Council, 'Summary of conclusions of the meeting of the JHA-RELEX Working Party (JAIEX) on 9 September 2011', 14th September 2011 (EU doc. no. 14174/11), p.6,

http://register.consilium.europa.eu/pdf/en/11/st14/st14174.en11.pdf

29. Internet Corporation for Assigned Names and Numbers, 'About',

http://www.icann.org/en/about/

30. MEMO/11/298, 'Neelie Kroes discusses Internet governance with US Administration', 13th May 2011,

http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/298&format=HTML&aged=0&language=EN&guiLanguage=en

31. General Secretariat of the Council, 'Summary of conclusions of the EU-US JHA Informal Senior Officials Meeting, Cracow, 25-26 July 2011', 29th July 2011, p.3,

http://register.consilium.europa.eu/pdf/en/11/st13/st13228.en11.pdf

This article was first published in Statewatch journal volume 21 no 4, March 2012