UNIVERSITY OF TORONTO

MUNK SCHOOL OF GLOBAL AFFAIRS

Join the Global Conversation

G7 Research Group

The
G7 Research Group
at the Munk School of Global Affairs at Trinity College in the University of Toronto
presents the

2016 Ise-Shima G7 Interim Compliance Report

29 May 2016 to 19 February 2017

Prepared by
Sarah Beard, Sophia Glisch, Humayun Ahmed, Katie Andrews and Sohaib Ahmed
with Brittaney Warren and Emily Scrivens
G7 Research Group, University of Toronto

15 April 2017
www.g7.utoronto.ca
g8@utoronto.ca
@g7_rg and @g8rg

"We have meanwhile set up a process and there are also independent institutions monitoring which objectives of our G7 meetings we actually achieve. When it comes to these goals we have a compliance rate of about 80%, according to the University of Toronto. Germany, with its 87%, comes off pretty well. That means that next year too, under the Japanese G7 presidency, we are going to check where we stand in comparison to what we have discussed with each other now. So a lot of what we have resolved to do here together is something that we are going to have to work very hard at over the next few months. But I think that it has become apparent that we, as the G7, want to assume responsibility far beyond the prosperity in our own countries. That's why today's outreach meetings, that is the meetings with our guests, were also of great importance."

Chancellor Angela Merkel, Schloss Elmau, 8 June 2015

Contents

8. International Cyber Stability

"We commit to promote a strategic framework of international cyber stability consisting of the applicability of existing international law to state behavior in cyberspace, the promotion of voluntary norms of responsible state behavior during peacetime, and the development and the implementation of practical cyber confidence building measures between states."

G7 Ise-Shima Leaders' Declaration

Assessment

	Lack of Compliance	Work in Progress	Full Compliance
Canada			+1
France			+1
Germany			+1
Italy		0	
Japan			+1
United Kingdom			+1
United States			+1
European Union			+1
Average		+0.88	

Background

While the term "cyberspace" can be interpreted in a range of ways, it can generally be defined as "the online world of computer networks and especially the Internet."[860] In the context of cyberspace and G7 commitments, it is important to understand how discussions of "cyberspace" have evolved from prior agreements and negotiations concerning information communication technologies (ICTs). ICTs are the "Internet technologies, infrastructure, applications and services" that connect individuals to the internet.[861]

ICTs and the role of the internet have previously been referenced at G7 and G8 summits, although prior summits focused predominantly on how to extend the economic and social benefits made available by the Internet to the general public. The Okinawa Charter on Global Information Society, for example, emphasized the importance of the "principle of inclusion," which is the idea that "everyone, everywhere should be enabled to participate in and no one should be excluded from the benefits of the global information society."[862] The 2011 G8 Deauville Summit's declaration furthered this discussion, with statements regarding the Internet and the importance of "coordination between governments, regional and international organizations, the private sector, civil society … to prevent, deter and punish the use of ICTs for terrorist and criminal purposes."[863] The importance of ICTs was again affirmed through the Charter for the Digitally Connected World, which was established before the 2016 G7 Ise-Shima Summit on 30 April 2016.[864]

[860] Cyberspace, Merriam-Webster Dictionary. Date of Access: November 7, 2016. http://www.merriam-webster.com/dictionary/cyberspace.
[861] Charter for the Digitally Connected World, G7/G8 Information Centre (Toronto) 30 April 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/ict/2016-ict-charter.html.
[862] Okinawa Charter on Global Information Society, G7/G8 Information Centre (Toronto) 22 July 2000. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm.
[863] G8 Declaration: Renewed Commitment for Freedom and Democracy, G7/G8 Information Centre (Toronto) 27 May 2011. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2011deauville/2011-declaration-en.html#internet.
[864] Charter for the Digitally Connected World, G7/G8 Information Centre (Toronto) 30 April 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/ict/2016-ict-charter.html.

The meetings leading up to the 2016 G7 Ise-Shima Summit marked the first time that G7 leaders made a clear commitment in the area of cybersecurity,[865] signifying the growing importance of cyber space, structure, and security for international governance.[866] While the commitment continues to emphasize the importance of topics such as the digital economy, human rights in cyberspace, and the role of ICTs in improving conditions around the world, what differentiates this "cyber" commitment from previous agreements and commitments concerned with ICTs is its specific focus on state behaviours in cyberspace. The obligation of state actors to regulate and coordinate their behaviours, with the explicit confirmation of international law's application to cyberspace, distinguishes the aims of the cyber commitment made at the Ise-Shima summit from previous commitments concerning ICTs and the Internet.

At the 2016 G7 Ise-Shima Summit, a new G7 working group was established to "enhance our policy coordination and practical cooperation to promote security and stability in cyberspace."[867] This occurred alongside the adoption of the G7 Principles and Actions on Cyber, which provide a concise description of the G7's aims of "promoting digital economy" alongside the social values that will accompany the growth of ICTs, while also "promoting security and stability in cyberspace" as described in the 2016 Ise-Shima commitment.[868]

Commitment Features

This commitment focuses on state behaviour and state interaction within cyberspace rather than on more technical areas (such as infrastructure-building or increasing accessibility). Given the normative element of this commitment, there are a number of actions that G7 members can take to comply. To help narrow the scope, it is necessary to consider the source of this commitment. The United States has taken a leadership role in this area, and has been "promoting a strategic framework of international cyber stability … [with] three key elements … (1) global affirmation of the applicability of international law to state behavior in cyberspace; (2) the development of international consensus on additional norms and principles of responsible state behavior in cyberspace that apply during peacetime; and (3) the development and implementation of practice CBMs [confidence building measures], which can help to ensure stability in cyberspace by reducing the risk of misperception and escalation."[869] Thus, the G7 commitment appears to have been heavily influenced by US policy.

The first element of this framework involves support for the idea that international law is applicable in cyber space. This is something which the G7 explicitly confirmed in the G7 Principles and Actions on Cyber.[870] Prior to this, it was affirmed by the 2013 United Nations Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GGE),[871] and later confirmed by the 2015 GGE.[872] GGEs are the

[865] Danielle Kriz and Mihoko Matsubara, In 2016, G7 Makes Cybersecurity a Priority and Paves the Way for Track 1.5 Multi-Stakeholder Discussions, Paloalto Networks (Santa Clara) 31 May 2016. Date of Access: 29 December 2016. http://researchcenter.paloaltonetworks.com/2016/05/cso-in-2016-g7-makes-cybersecurity-a-priority-and-paves-the-way-for-track-1-5-multi-stakeholder-discussions/.
[866] G7 Ise-Shima Leaders' Declaration, G7/G8 Information Centre (Toronto) 27 May 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber.
[867] G7 Ise-Shima Leaders' Declaration, G7/G8 Information Centre (Toronto) 27 May 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber.
[868] G7 Principles and Actions on Cyber, G7/G8 Information Centre (Toronto) 27 May 2-16. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2016shima/cyber.html.
[869] Department of State International Cyberspace Policy Strategy, Department of State (Washington DC) March 2016. Date of Access: 20 November 2016.
[870] G7 Principles and Actions on Cyber, G7 Information Centre (Toronto) 27 May 2016. Date of Access: 20 November 2016. http://www.g8.utoronto.ca/summit/2016shima/cyber.html.
[871] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations (New York) 24 June 2013. Date of Access: 20 November 2016. https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf.

main instrument that the international community has used to discuss international law's applicability to cybersecurity, though their reports are non-binding.[873] While statements confirming the applicability of international law to cybersecurity are one means by which G7 states could comply with this aspect of the commitment, G7 members have also noted that they "look forward to the work of the new GGE, including further discussions on how existing international law applies to cyberspace."[874] Thus, participation in the 2016 GGE or other initiatives with the goal of enhancing dialogue in this area could also count towards compliance.

The second element of this commitment requires that G7 members to take steps to support a framework that involves "the promotion of voluntary norms of responsible state behavior during peacetime."[875] Although the G7 does not clearly define what these norms are, they do "reaffirm that no country should conduct or knowingly support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to its companies or commercial sectors."[876] The US has labelled this commitment such a norm and called for its adoption in the past.[877] Thus, compliance with this part of the commitment requires the G7 member to make efforts to affirm and uphold this norm or others like it.

The last element of this commitment involves a pledge by G7 members to take steps to support an international cyber stability framework that involves the "development and the implementation of practical cyber confidence building measures between states."[878] This aspect of the commitment was affirmed by the 2015 UN GGE Report, which recommended "the development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations" in the area of ICTs.[879] The US has noted that "examples of cyber CBMs include: transparency measures, such as sharing national strategies or doctrine; cooperative measures, such as an initiative to combat a particular cyber incident or threat actor; and stability measures, such as committing to refrain from a certain activity of concern."[880] In addition, parties to the Organization for Security and Co-operation in Europe (OSCE), which includes the G7 members, agreed on a clear set of CBMs in March 2016.[881] Therefore, examples of compliance could include, but are not limited to, agreements

[872] Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations Office for Disarmament Affairs (New York). Date of Access: 20 November 2016. https://www.un.org/disarmament/topics/informationsecurity/.
[873] Elaine Korzak, Cybersecurity at the UN: Another Year, Another GGE, Lawfare, 10 December 2015. Date of Access: 20 November 2016. https://www.lawfareblog.com/cybersecurity-un-another-year-another-gge.
[874] G7 Principles and Actions on Cyber, G7 Information Centre (Toronto) 27 May 2016. Date of Access: 20 November 2016. http://www.g8.utoronto.ca/summit/2016shima/cyber.html.
[875] G7 Ise-Shima Leaders' Declaration, G7/G8 Information Centre (Toronto) 27 May 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber.
[876] G7 Ise-Shima Leaders' Declaration, G7/G8 Information Centre (Toronto) 27 May 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber.
[877] Statement by US Legal Adviser Brian J. Egan at Berkeley Law School, US Department of State (Berkeley) 10 November 2016. Date of Access: 20 November 2016. https://www.state.gov/s/l/releases/remarks/264303.htm.
[878] G7 Ise-Shima Leaders' Declaration, G7/G8 Information Centre (Toronto) 27 May 2016. Date of Access: 25 September 2016. http://www.g8.utoronto.ca/summit/2016shima/ise-shima-declaration-en.html#cyber.
[879] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (Geneva) 22 July 2015. Date of Access: 25 September 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
[880] International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms, US Department of State (Washington DC) 25 May 2016. Date of Access: 20 November 2016. https://www.state.gov/s/cyberissues/releasesandremarks/257719.htm.
[881] Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming From the Use of Information and Communication Technology, Organization for Security and Co-Operation in Europe Permanent Council, 10 March 2016. Date of Access: 21 November 2016. https://ccdcoe.org/sites/default/files/documents/OSCE-160310-NewCBMs.pdf.

referring to cyber cooperation or cybersecurity building, information-sharing measures, measures increasing transparency on cyber policy, the promotion of public-private partnerships, or measures to increase awareness about the security of industrial infrastructure.

To fully comply with this commitment, G7 members must take action in all three areas. Members who take action in only one or two of these areas will be considered to have partially complied with the commitment and will be given a score of 0. Members who do not take action in any of the three areas specified by the commitment, or take actions that seriously undermine any of the areas will have failed to comply with the commitment, and will be assigned a score of –1.

Scoring Guidelines

–1	Member fails to take steps to promote the application of international law in cyberspace AND does not support "the promotion of voluntary norms of responsible state behavior during peacetime" AND takes no confidence building measures to strengthen cyberspace stability.
0	Member takes steps to promote the application of international law in cyberspace OR supports "the promotion of voluntary norms of responsible state behavior during peacetime" OR takes confidence building measures to strengthen cyberspace stability.
+1	Member takes steps to promote the application of international law in cyberspace AND supports "the promotion of voluntary norms of responsible state behavior during peacetime" AND takes confidence building measures to strengthen cyberspace stability.

Lead Analyst: Eimi Harris

Canada: +1

Canada has fully complied with its commitment to promote a strategic framework for international cyber stability.

On 27 May 2016, in a shortened response to the United Nation's resolution 70/237, the Government of Canada informed the UN Secretary General that the Canadian government believes existing international law should be applicable to a state's use of information and communications technologies.[882] The Canadian government also recognized that a robust framework of peacetime norms helps facilitate an international order in which states are able to support a stable cyberspace.[883] Finally, the Canadian government expressed its belief in confidence building measures, as they are a proven method to reducing tensions and the risk of conflict.[884]

On 29 June 2016, Prime Minister Justin Trudeau released a press statement outlining the Canadian position on the major talking points of the 2016 North American Leaders' Summit. On the subject of cybersecurity, Prime Minister Trudeau noted that "[Canada] commits to promoting stability in cyberspace based on the applicability of international law, voluntary norms of responsible state behaviour during peacetime, and practical confidence building measures between states."[885] In particular, he wrote that "no country should conduct or knowingly support cyber-enabled theft of intellectual property, including trade secrets or other confidential business information, with the

[882] Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly (New York) 19 July 2016. Date of Access: 10 January 2017. http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172

[883] Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly (New York) 19 July 2016. Date of Access: 10 January 2017. http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172

[884] Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly (New York) 19 July 2016. Date of Access: 10 January 2017. http://www.un.org/ga/search/view_doc.asp?symbol=A/71/172

[885] 2016 North American Leaders' Summit, Office of the Prime Minister of Canada (Ottawa) 29 June 2016. Date of Access: 10 January 2017. http://pm.gc.ca/eng/news/2016/06/29/regional-and-global-issues-2016-north-american-leaders-summit

intent of providing competitive advantages to its companies or commercial sectors"[886] and that "every country should cooperate, consistent with its domestic laws and international obligations, with requests for assistance from other states in mitigating malicious cyber activity emanating from its territory."[887]

On 5 August 2016, Canada published its official Cyber Security Strategy, in which the government announced that it will help less developed states and foreign partners develop cyber security capacities.[888] In addition, Canada will continue to take part in training and exercise programs on the topic of cyber security, which the Canadian government believes will help improve the understanding of the dynamics among cyber security partners.[889]

On 16 October 2016, a consultation published by the Government of Canada outlined key action areas moving forward on the issue of cyber. Recognizing the "importance of cyber security for businesses, economic growth, and prosperity,"[890] the Canadian government's first key action area was entitled "Resilience." By certifying businesses that meet cyber security standards and by encouraging executives in private sector companies to report on the cyber security health of their organizations, the Government of Canada hopes to better prevent, mitigate, and respond to cyber attacks targeting Canadian corporations.[891] This would also establish a normative structure consistent with the UN Group of Governmental Expert's 2015 cyber stability report, ensuring the "integrity of the supply chain so that end users can have confidence in the security of ICT products"[892] as well as encouraging "responsible reporting of ICT vulnerabilities."[893]

Canada has made several efforts to promote the applicability of international law in cyberspace, advocate for a system of peacetime cyberspace norms, and take confidence building measures to strengthen cyberspace stability, and has thus been awarded a score of +1.

Analyst: Bill Xu

France: +1

France has fully complied with this commitment.

[886] 2016 North American Leaders' Summit, Office of the Prime Minister of Canada (Ottawa) 29 June 2016. Date of Access: 10 January 2017. http://pm.gc.ca/eng/news/2016/06/29/regional-and-global-issues-2016-north-american-leaders-summit
[887] 2016 North American Leaders' Summit, Office of the Prime Minister of Canada (Ottawa) 29 June 2016. Date of Access: 10 January 2017. http://pm.gc.ca/eng/news/2016/06/29/regional-and-global-issues-2016-north-american-leaders-summit
[888] Canada's Cyber Security Strategy, Public Safety Canada (Ottawa) 5 August 2017. Date of Access: 10 January 2017. http://www.securitepubliquecanada.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.
[889] Canada's Cyber Security Strategy, Public Safety Canada (Ottawa) 5 August 2017. Date of Access: 10 January 2017. http://www.securitepubliquecanada.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/index-en.aspx.
[890] Security and Prosperity in the Digital Age, Public Safety Canada (Ottawa) 16 October 2016. Date of Access: 10 January 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx.
[891] Security and Prosperity in the Digital Age, Public Safety Canada (Ottawa) 16 October 2016. Date of Access: 10 January 2017. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-scrty-prsprty/index-en.aspx.
[892] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly (New York) 22 July 2015. Date of Access: 16 January 2017. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174
[893] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly (New York) 22 July 2015. Date of Access: 16 January 2017. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

On 28 September 2016, France introduced the "Loi Numérique." [894] The law established the Internet as being a fundamental right for French people four years after the UN recognized it as such.[895] This has also been promoted as an initiative for increased access to data and transparency, which was written into France's digital strategy in 2015.[896] These two elements contribute to the application of international law and norm-building in cyberspace.

On 7 October 2016, the "Loi pour une Republique Numérique," which aimed to increase transparency and democratize cyberspace, was adopted.[897] The law's mandate is structured around liberty (the freedom to innovate), equality (the promotion of confidence building measures) and fraternity (the increased inclusivity of cyberspace).[898] The second theme focuses on protecting individuals and businesses from having their information compromised by strengthening the country's cyberdefense apparatuses, as recommended in the latest report of the United Nations Group of Governmental Experts (GGE). [899]

On 18 October 2016, President of the Assemblée Nationale Elisabeth Guigou suggested revamping France's cybersecurity strategy amidst an exponential increase in cyberattacks (up to 400 per second) and suggested a state-wide and Europe-wide coordinated efforts to combat cyber threats.[900]

On 14 December 2016, one report out of the Assemblée Nationale proposed that the 23 November 2001 Budapest convention be adapted to consider a climate of increased cybercriminality and terrorism seen across Europe.[901] This can be interpreted as following a norm described by the UN GGE that "states should cooperate in developing and applying measures to increase stability and security in the use of ICTs [information and communications technologies] and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security."[902]

On 13 January 2017, France and Canada signed a Declaration of Intent to continue to promote the applicability and protection of human rights pursuant to the G7 Principles and Actions on Cyber. This bilateral agreement opens the door for further military and intelligence cooperation and cites Da'esh as a target of their conjoined efforts.[903] This is in accordance with norms around cooperating

[894] Loi numérique: Internet devient enfin un droit fondamental en France (Paris). 29 September 2016. Date of Access: 8 January 2017. http://hightech.bfmtv.com/epoque/loi-numerique-internet-devient-enfin-un-droit-fondamental-en-france-1042491.html.

[895] UN report declares internet access a human right (San Francisco). 6 June 2011. Date of Access: 17 January 2017. https://www.wired.com/2011/06/internet-a-human-right/.

[896] French National Digital Security Strategy (Brussels). 16 October 2015. Date of Access: 3 January 2017. https://www.enisa.europa.eu/topics/national-cyber security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf.

[897] Le projet de loi numerique adopte (Paris). 28 September 2016. Date of Access: 8 January 2017. http://www.lefigaro.fr/flash-actu/2016/09/28/97001-20160928FILWWW00258-le-projet-de-loi-numerique-adopte.php.

[898] Egalite des droits: la confiance, socle de la societe numerique (Paris). Date of Access: 18 January 2017. http://www.gouvernement.fr/egalite-des-droits-la-confiance-socle-de-la-societe-numerique-2402.

[899] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (New York). 22 July 2015. Date of Access: 18 January 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[900] Commission des affaires etrangeres (Paris). 18 October 2016. Date of Access: 5 January 2017. http://www.assemblee-nationale.fr/14/cr-cafe/16-17/c1617007.asp.

[901] Rapport fait au nom de la commission des lois constitutionnelles, de la législation et de l'administration générale de la République sur la proposition de la résolution Européenne (N°4268) sur la proposition franco-allemande d'un "pacte de sécurité européen" (Paris). 14 December 2016. Date of Access : 9 January 2017. http://www.assemblee-nationale.fr/14/rapports/r4310.asp.

[902] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (New York). 22 July 2015. Date of Access: 18 January 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.

[903] Canada-France Enhanced Cooperation Agenda (Ottawa). 13 October 2016. Date of Access: 18 January 2017. http://pm.gc.ca/eng/news/2016/10/13/canada-france-enhanced-cooperation-agenda.

to exchange information and respecting the application of human rights in cyberspace, as described in the 2015 UN GGE Report.[904]

France's initiatives focused on treating the human right to online access, opening a dialogue about state-wide and regional efforts governing cyberspace and making its digital infrastructure less prone to cyberattacks that could undermine the public and enterprises' information — two elements that speak to the applicability of international law in cyberspace and norm-building on the support of critical infrastructure against cyberattacks. France also took confidence building measures to strengthen cyber stability. Thus, France has fully complied with the commitment and has been awarded a score of +1.

Analyst: Helena Najm

Germany: +1

Germany has fully complied with its commitment to promote international law in cyberspace, support common norms in state behaviour and encourage international communication. The German government has shared its plans and goals for national and international cyber security with the public. Germany's plan to launch an emergency response team in the case of attacks on federal authorities and critical enterprises highlights the country's strong stance on responsible state behaviour and intolerance for the theft of intellectual property through information and communications technologies. The plan to develop a German institute for international cyber security in which all international and cross-sector parties can exchange information and questions shows the government's commitment to cyber cooperation and to further enhancing dialogue.

On 9 June 2016, the German Federal Office for Information Security Technology published its plan to introduce a "cyber fire department" in order to deal with cyber attacks on the federal administration and operators of critical infrastructures.[905] The project will launch in 2017 under the title "Mobile Incident Response Teams" and will help the affected authorities and enterprises to stabilize and restructure their information technology infrastructures.[906] The United Nations had previously outlined in the 2015 report of the United Nations Group of Governmental Experts that there is a normative expectation for states to protect their critical infrastructure from possible cyber attacks.[907]

During the Warsaw Summit of the North Atlantic Treaty Organization (NATO) on 8-9 July 2016, Germany committed itself, together with its fellow NATO members, to the implementation of NATO's long Enhanced Policy on Cyber Defence. The process will be conducted in accordance with international law and by following "the principle of restraint and support maintaining international peace, security, and stability in cyberspace."[908] In her press release from the NATO meeting on 8 July 2016, Chancellor Angela Merkel stressed the importance of the planned creation of an international

[904] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (New York). 22 July 2015. Date of Access: 18 January 2016. http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174.
[905] "BSI: Cyber-Feuerwehr" für grosse Hackerangriffe soll 20 Personen umfassen" Heise Online, 9 June 2016. Date of Access: 11 January 2017. https://www.heise.de/newsticker/meldung/BSI-Cyber-Feuerwehr-fuer-grosse-Hackerangriffe-soll-20-Personen-umfassen-3234170.html.
[906] "BSI: Cyber-Feuerwehr" für gros1e Hackerangriffe soll 20 Personen umfassen" Heise online, 9 June 2016. Access: 11 January 2017. https://www.heise.de/newsticker/meldung/BSI-Cyber-Feuerwehr-fuer-grosse-Hackerangriffe-soll-20-Personen-umfassen-3234170.html.
[907] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations (New York) 24 June 2013. Date of Access: 20 November 2016. https://ccdcoe.org/sites/default/files/documents/UN-130624-GGEReport2013_0.pdf.
[908] Voltaire Network, "NATO Warsaw Summit Communiqué" Voltaire Network, Section 70, 9 July 2016. Access: 11 January 2017. http://www.voltairenet.org/article192794.html.

cyberspace task force within NATO.[909] This action addresses both the application of international law in cyberspace and efforts to introduce confidence building measures between states.

On 9 November 2016, the Federal Government of Germany passed the Sicherheitsstrategie für Deutschland 2016 ("Security Strategy for Germany 2016). The plan outlines Germany's goal to create interoperable cyber security architectures and standards and to further shape the supplement and application of international law in the cyber sphere.[910] Additionally, it outlines the foundation of a German institute for international cyber security.[911] This action falls within efforts to apply international law in cyberspace and introduce confidence building measures between states

Germany has started to take the necessary steps to fulfill the requirements of this commitment. Overall, the German government has achieved items that fulfill criteria around international law, normative development, and confidence building measures. Thus, Germany has been awarded a score of +1.

Analyst: Friederike Wilke

Italy: 0

Italy has partially complied with its commitment to cyber stability. Since the Ise-Shima Summit took place in May 2016, Italy has taken actions towards the promotion of voluntary norms of responsible state behaviour during peacetime and implementing practical confidence building measures between states. However, it has not taken visible action on confirming the applicability of existing international law.

On 29 September 2016, Alessandro Pansa, Director General of the Department of Security Intelligence, made a speech at the CyberTech Europe conference referencing Italy's efforts on its national cybersecurity strategy.[912] His speech highlighted the importance of protecting critical infrastructure from cyberattacks, referencing Italy's efforts to align its National Plan for Cyber Security and Internet Safety to the EU Directive on Network and Information Security, as well as suggesting ideas for the testing of cyber systems for vulnerabilities before implementing them in critical infrastructure.[913]

On 7-9 December 2016, representatives from the Agenzia per l'Italia Digitale (Agency for Italy Digital) and the Department of Public Service took part in the international summit hosted by the Open Government Partnership.[914] Prior to participating in this summit, Italy published its third Action Plan on 20 September 2016. The Action Plan referenced the importance of cooperating with

[909] Die Bundesregierung, "Pressestatement von Bundeskanzlerin Dr. Angela Merkel anlässlich des NATO-Gipfels am 8. Juli 2016", 8 July 2016. Access: 11 January 2017. https://www.bundesregierung.de/Content/DE/Mitschrift/Pressekonferenzen/2016/07/2016-07-08-statement-merkel-warschau.html.

[910] Bundesministerium des Innern, "Cyber-Sicherheitsstrategie für Deutschland", page 41. Access: 11 January 2016. http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

[911] Bundesministerium des Innern, "Cyber-Sicherheitsstrategie für Deutschland", page 41. Access: 11 January 2016. http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

[912] Pansa: per l'Italia un progetto forte di cybersecurity, Sistema di Informazione per la Sicurezza della Repubblica, 29 September 2016. Date of Access: 21 January 2017. https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pansa-per-litalia-un-progetto-forte-di-cybersecurity.html

[913] Pansa: per l'Italia un progetto forte di cybersecurity, Sistema di Informazione per la Sicurezza della Repubblica, 29 September 2016. Date of Access: 21 January 2017. https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/pansa-per-litalia-un-progetto-forte-di-cybersecurity.html

[914] AgID a Parigi per l'Open Government Partners Summit, Agenzia per l'Italia Digitale, 7 December 2016. Date of Access: 21 January 2017. http://www.agid.gov.it/notizie/2016/12/07/agid-parigi-lopen-government-partnership-global-summit.

businesses, citizens, and other governments to promote transparency and accountability while preventing corruption.[915]

On 20 December 2016, the Bank of Italy signed an agreement with the Italian Banking Association and the ABI Lab Consortium to strengthen collaboration on cybersecurity between Italian and global banking firms and financial operators.[916] This agreement specifically creates CERTFin, a computer emergency response team, and, as referenced in the press release, is "in line with the [Italian] National Strategic Framework for the Security of Cyberspace" on initiatives such as critical infrastructure protection and cooperative efforts between institutional partners, national experts, and international experts.[917]

On 12 January 2017, the Italian Minister for the Interior Marco Minniti met with European Commissioner for Migration, Home Affairs, and Citizenship Dimitris Avramopoulous.[918] A joint press release alluded to discussions around cybersecurity cooperation between the EU and Italy for security purposes. Specifically, "discussions focused mainly on strengthening cooperation in the areas of counter-terrorism as well as information exchange, radicalisation and cybersecurity. Italy is committed to working with European partners to achieve a genuine and effective Security Union."[919]

Despite having taken action in the realm of cyberspace that promotes the voluntary norms of responsible state behaviour and confidence building measures in cyberspace, Italy has achieved only partial compliance with this commitment because it has not taken visible steps in terms of the applicability of international law. Thus, Italy receives a score of 0.

Analyst: Eimi Harris

Japan: +1

Japan has fully complied with its commitment to cyber stability. Through a series of bilateral and multilateral negotiations, Japan's Ministry of Foreign Affairs has been actively coordinating strategies for cyberspace with other countries and addressing all three major elements of the commitment to cyber stability (the application of international law to cyberspace, the promotion of norms for states in cyberspace, and confidence building measures between states for cyberspace). However, Japan has not elaborated enough on the actions that it will take under these initiatives to achieve full compliance.

On 12 July 2016, the Ministry of Foreign Affairs announced the establishment of the Cyber Security Policy Division.[920] The ministry will use the Division, which will be housed under the National Security Policy Division in the Foreign Policy Bureau, to "continue to actively conduct foreign policy

[915] Open Government in Italia: 3rd Piano d'azione 2016-2018, Ministro per la Semplificazione e la Pubblica Amministrazione, Open Government Partnership, 20 September 2016. Date of Access: 21 January 2017. http://open.gov.it/wp-content/uploads/2016/09/2016-09-23-Terzo-Piano-Azione-OGP-Nazionale-FinaleDEF_m.pdf
[916] The Bank of Italy and ABI sign an agreement to enhance cybersecurity, The Bank of Italy (Rome) 20 December 2016. Date of Access: 22 January 2017. http://www.bancaditalia.it/media/comunicati/documenti/2016-02/en-cs20161220-bi-abi.pdf?language_id=1
[917] The Bank of Italy and ABI sign an agreement to enhance cybersecurity, The Bank of Italy (Rome) 20 December 2016. Date of Access: 22 January 2017. http://www.bancaditalia.it/media/comunicati/documenti/2016-02/en-cs20161220-bi-abi.pdf?language_id=1
[918] Joint Statement by Commissioner Dimitris Avramopoulos and Italian Minister for the Interior Marco Minniti following their meeting in Rome, Statement/17/56, European Commission (Rome) 12 January 2017. Date of Access: 22 January 2017. http://europa.eu/rapid/press-release_STATEMENT-17-56_en.htm?locale=en.
[919] Joint Statement by Commissioner Dimitris Avramopoulos and Italian Minister for the Interior Marco Minniti following their meeting in Rome, Statement/17/56, European Commission (Rome) 12 January 2017. Date of Access: 22 January 2017. http://europa.eu/rapid/press-release_STATEMENT-17-56_en.htm?locale=en.
[920] Establishment of Cyber Security Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan, 12 July 2016. Date of Access: 22 January 2017. http://www.mofa.go.jp/press/release/press4e_001203.html.

in the field of cyber from a comprehensive perspective, especially promoting the rule of law in cyberspace, confidence building, and capacity building of developing countries."[921]

On 27 July 2016, Japan and the United States conducted their fourth Cyber Dialogue in Washington DC.[922] The meeting was to build on the third Japan-US Cyber Dialogue from July 2015 and would address "a wide range of Japan-US cooperation on cyber issues, including situational awareness, critical infrastructure protection and bilateral cooperation in the international arena, including capacity building."[923] In discussions, "both sides also committed to maintain their dialogue and to continue to enhance the importance of cyber issues in our bilateral cooperation."[924]

On 2 August 2016, Japan and Australia conducted their second Cyber Policy Dialogue in Tokyo.[925] Building off the first Cyber Policy Dialogue from 2014, Japan and Australia "reaffirmed their cooperation on the elaboration of international law and norms, and confidence building measures in international and regional fora such as UNGGE [United Nations Group of Governmental Experts] and ASEAN [Association of Southeast Asian Nations] Regional Forum."[926] The two countries also discussed joint efforts to manage regional cyber threats through capacity building and joint exercises.

On 13 October 2016, Japan and the United Kingdom held their third bilateral consultations on Cyberspace in Tokyo.[927] Their discussions were centred on "bilateral cooperation on various issues such as critical infrastructure protection and capacity building as well as … collaboration at various fora such as the United Nations."[928]

On 20 December 2016, experts from Japan, the United States, and Korea conducted a meeting on cybersecurity of critical infrastructure.[929] At this meeting, representatives from the Foreign Affairs departments from each country "exchanged opinions over the current environment and threats in the field of cybersecurity of critical infrastructure" and promised continued trilateral cooperation on issues of cybersecurity.[930]

Japan has been very active in engaging with other states on the key topic of cyber stability; the application of international law to cyberspace, the promotion of norms for states in cyberspace, and confidence building measures between states for cyberspace were all addressed throughout these bilateral and multilateral meetings. Japan has thus fully complied with the commitment and thus receives a score of +1.

Analyst: Eimi Harris

[921] Establishment of Cyber Security Policy Division, Foreign Policy Bureau, Ministry of Foreign Affairs of Japan, 12 July 2016. Date of Access: 22 January 2017. http://www.mofa.go.jp/press/release/press4e_001203.html.
[922] The 4th Japan-US Cyber Dialogue, Ministry of Foreign Affairs of Japan, 27 July 2016. Date of Access: 21 January 2017. http://www.mofa.go.jp/press/release/press4e_001218.html.
[923] The 4th Japan-US Cyber Dialogue, Ministry of Foreign Affairs of Japan, 27 July 2016. Date of Access: 21 January 2017. http://www.mofa.go.jp/press/release/press4e_001218.html.
[924] The Fourth Annual U.S.-Japan Cyber Dialogue, U.S. Pacific Command (USPACOM), 15 September 2016. Date of Access: 22 January 2017. http://www.pacom.mil/Media/News/News-Article-View/Article/945940/the-fourth-annual-us-japan-cyber-dialogue/.
[925] The 2nd Japan-Australia Cyber Policy Dialogue, Ministry of Foreign Affairs of Japan, 8 August 2016. Date of Access: 21 January 2017. http://www.mofa.go.jp/a_o/ocn/au/page4e_000484.html.
[926] The 2nd Japan-Australia Cyber Policy Dialogue, Ministry of Foreign Affairs of Japan, 8 August 2016. Date of Access: 21 January 2017. http://www.mofa.go.jp/a_o/ocn/au/page4e_000484.html.
[927]The 3rd Japan-UK bilateral Consultations on Cyberspace, Ministry of Foreign Affairs of Japan, 13 October 2016. Date of Access: 22 January 2017. http://www.mofa.go.jp/press/release/press4e_001308.html.
[928]The 3rd Japan-UK bilateral Consultations on Cyberspace, Ministry of Foreign Affairs of Japan, 13 October 2016. Date of Access: 22 January 2017. http://www.mofa.go.jp/press/release/press4e_001308.html.
[929] Japan-US-ROK Experts Meeting on Cybersecurity of Critical Infrastructure, Ministry of Foreign Affairs of Japan, 20 December 2016. Date of Access: 22 January 2017. http://www.mofa.go.jp/press/release/press4e_001419.html.
[930] Japan-US-ROK Experts Meeting on Cybersecurity of Critical Infrastructure, Ministry of Foreign Affairs of Japan, 20 December 2016. Date of Access: 22 January 2017. http://www.mofa.go.jp/press/release/press4e_001419.html.

United Kingdom: +1

The United Kingdom has fully complied with its commitment at the 2016 Ise-Shima Summit to promote international cyber stability and apply international law, endorse state-level normative behaviour and create confidence building measures in regards to cyberspace.

On 13 June 2016, representatives of the United Kingdom met with their counterparts from China to discuss state security. At these meetings, the Chinese and British participants outlined the normative behaviour that both states would adhere to in regards to cyber security. Both China and the UK pledged to "hold discussions on combatting cyber crime … and cyber security … with the aim of sharing intelligence and experience."[931] They also promised to "increase cooperation on cyber security related incidents … agreeing to respond promptly to any request for information or assistance."[932]

On 30 September 2016, the United Kingdom announced that the National Cyber Security Centre would become operational on 3 October 2016.[933] The centre is tasked with four main objectives: to "understand the cyber security environment," "reduce [cyber] risks to the UK," "nurture and grow … national cyber security capability," and "respond to cyber security incidents."[934] It purports that it will "work collaboratively" with "international partners" to tackle cyber security.[935] The centre did not address how it will engage with its international partners, or who those international partners are, but did state that the centre will "engag[e] with international partners on incident handling, situational awareness, building technical capabilities and capacity … and contributing to broader cyber security discussions."[936]

On 1 November 2016, the Chancellor of the Exchequer, Philip Hammond, announced the 2016-2021 National Cyber Security Strategy.[937] It is based on three main strategic pillars — defend, deter and develop — and includes the objectives and approaches the government seeks to utilize in order to promote international cooperation and to integrate international law into the field of cyber security. The report stated that the government would ensure that "international law applies in cyberspace," that "voluntary, non-binding, norms of responsible state behaviour" were upheld, and that they would promote "the development and implementation of confidence building measures."[938] The UK has promised to supplement the program with GBP1.9 billion in investment.[939]

[931] China-UK High Level Security Dialogue: Communique (Online) 13 June 2016. Date of Access: 17 January 2017. https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.
[932] China-UK High Level Security Dialogue: Communique (Online), 13 June 2016. Date of Access: 17 January 2017. https://www.gov.uk/government/publications/china-uk-high-level-security-dialogue-official-statement/china-uk-high-level-security-dialogue-communique.
[933] NCSC - The National Cyber Security Centre becomes operational (Online), 3 October 2016. Date of Access: 12 January 2017. https://www.ncsc.gov.uk/news/national-cyber security-centre-becomes-operational.
[934] Prospectus Introducing the National Cyber Security Centre (Online), 25 May 2016. Date of Access: 12 January 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf.
[935] NCSC – About Us (Online), Date Accessed: 12 January 2017. https://www.ncsc.gov.uk/about-us.
[936] Prospectus Introducing the National Cyber Security Centre (Online), 25 May 2016, Date of Access: 12 January 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf.
[937] Chancellor speech: launching the National Cyber Security Strategy (Online), 1 November 2016, Date of Access: 12 January 2017. https://www.gov.uk/government/speeches/chancellor-speech-launching-the-national-cyber-security-strategy.
[938] National Cyber Security Strategy 2016 to 2021 (Online), 1 November 2016, Date of Access: 12 January 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
[939] National Cyber Security Strategy 2016 to 2021 (Online), 1 November 2016, Date of Access: 12 January 2017. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.

Having successfully implemented policies that promote the application of international law in cyberspace, engaged in the creation of normative state behaviour in regards to cyber security and cooperation, and enabled the creation of confidence building measures designed to foster a more amicable and cooperative international cyber environment, the United Kingdom has fully complied with its commitment on cyber stability and receives a score of +1.

Analyst: Nick Allard

United States: +1

The United States has fully complied with its commitment to implement and promote a strategic framework for increasing international cyber stability.

On 3 June 2016, Christopher Painter, US State Department Coordinator for Cyber Issues, gave a TED talk in which he repeated the commitments agreed to during the Ise-Shima Summit and discussed how the United States was approaching these commitments.[940] Painter emphasized that State Department officials were engaging with diplomats in countries whose code of conduct in cyberspace is deemed unacceptable. Similarly, they are engaging with diplomats in other countries to make them aware of the behaviour expected of States in cyberspace.

On 29 June 2016, the United States held bilateral diplomatic consultations on the topic of cyber stability with Korea.[941] The consultations reaffirmed cooperation between Korea and the United States on international cybersecurity, capacity building and information sharing. It also reaffirmed their commitments to shared principles that support open and secure international cyberspace.

On 19 September 2016, the State Department spoke to a Presidential Commission on Enhancing National Cybersecurity and reaffirmed its policy of promoting the applicability of international law in cyberspace, voluntary norms of responsible state behaviour in cyberspace and confidence building measures between states.[942]

Between 10 October 2016 and 12 October 2016, Christopher Painter travelled to Singapore to represent the United States at the inaugural Singapore International Cyber Week.[943] He delivered a keynote address on international law and cyberspace, and on open and secure international cyberspace.

On 13 October 2016, Christopher Painter travelled to Japan for the inaugural meeting of the Group of Seven Ise-Shima Cyber Group, a working group created at the 2016 G7 summit.[944] The meeting aimed to enhance policy coordination between G7 members on cybersecurity and stability.

On 19 December 2016, the United States held trilateral talks with Japan and Korea.[945] The purpose of these talks was to discuss potential threats to international cyber infrastructure and advance cooperation on cybersecurity.

[940] Tedx Tysons Talk, U.S. Department of State (Washington, D.C.) 3 June 2016. Date of Access: 11 January 2017. https://www.state.gov/s/cyberissues/releasesandremarks/264041.htm.
[941] The 4th U.S.-Republic of Korea Bilateral Cyber Consultations, U.S. Department of State (Washington, D.C.) 29 June 2016. Date of Access: 11 January 2017. https://www.state.gov/r/pa/prs/ps/2016/06/259197.htm.
[942] Statement Before the Presidential Commission on Enhancing National Cybersecurity, U.S. Department of State (Washington, D.C.) 19 September 2016. Date of Access: 11 January 2017. https://www.state.gov/s/cyberissues/releasesandremarks/262204.htm.
[943] Coordinator for Cyber Issues Christopher Painter Travels to Singapore and Japan for High Level meetings on Cyber Issues, U.S. Department of State (Washington, D.C.) 7 October 2016. Date of Access: 11 January 2017. https://www.state.gov/r/pa/prs/ps/2016/10/262924.htm.
[944] Coordinator for Cyber Issues Christopher Painter Travels to Singapore and Japan for High Level meetings on Cyber Issues, U.S. Department of State (Washington, D.C.) 7 October 2016. Date of Access: 11 January 2017. https://www.state.gov/r/pa/prs/ps/2016/10/262924.htm.

Between 6 December 2016 and 9 December 2016, US representatives attended the 2016 Internet Governance Forum and reiterated the government's desire to build coalitions on the matter of cyber security and Internet governance.[946]

These examples show that the United States has made efforts towards affirming the application of international law in cyberspace, promoting the building of norms around state behaviour in cyberspace, and taking confidence building measures within cyberspace. The United States has fully complied with its commitment to promoting international cyber security and, thus, receives a score of +1.

Analyst: Syed Raza

European Union: +1

The European Union has fully complied with its commitment to cyber stability through the application of international law within cyberspace, promotion of voluntary norms of responsible state behaviour during peacetime, and establishment of confidence building measures.

On 28 June 2016, the 2016 EU Global Strategy report was released. This report outlines the EU's principles and goals within the global context.[947] The report states that the EU will strive towards executing "cyber diplomacy" and "digital governance" while engaging in agreements with its allies in using the guiding principles of international law to initiate responsible state behavior in cyberspace.[948] This dialogue also corresponds with the application of international law to cyberspace and the promotion of voluntary norms for responsible state behavior during peacetime.

On 6 July 2016, the European Parliament adopted the Directive on Security of Network and Information Systems (NIS), the first ever EU-wide legislation addressing cybersecurity.[949] The directive contains legal actions to increase the level of cybersecurity by prompting companies in sectors such as transport, energy, health and banking to adopt risk management considerations in the digital economy.[950] Member states are required to be appropriately equipped during cyber incidents with a Computer Security Incident Response Team (CSIRT) and a national NIS authority, while also setting up a cooperation group to oversee the strategic exchange of information among all member states and a CSIRT network to facilitate collaboration on cybersecurity occurrences.[951]

On 5 August 2016, an earlier framework of cooperation between the EU and Canada was upgraded, further embracing their democratic values. This agreement states that the parties acknowledge that cybercrime is a global problem and will work collaboratively to aid other states in developing effective

[945] U.S.-ROK-Japan Experts Meeting on Cybersecurity of Critical Infrastructure, U.S. Department of State (Washington D.C.) 19 December 2016. Date of Access: 17 January 2017. https://www.state.gov/r/pa/prs/ps/2016/12/265783.htm.
[946] U.S. Government Participation at the 2016 Internet Governance Forum, U.S. Department of State (Washington, D.C.) 5 December 2016. Date of Access: 11 January 2017. https://www.state.gov/r/pa/prs/ps/2016/12/264832.htm.
[947] A Global Strategy on Foreign and Security Policy for the European Union, Europa (Brussels) June 2016. Date of Access: 19 January 2017. https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union.
[948] EU Global Strategy: Shared Vision, Common Action: A Stronger Europe, European Commission (Brussels) 2016. Date of Access: 19 January 2016. https://eeas.europa.eu/top_stories/pdf/eugs_review_web.pdf
[949] The Directive on Security of Network and Information Systems (NIS Directive), Digital Single Market. 28 July 2016. Date of Access: 14 January 2017. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.
[950] Statement by Vice-President Ansip and Commissioner Oettinger Welcoming the Adoption of the First EU-Wide Rules on Cybersecurity, Europa (Brussels) 6 July 2016. Date of Access: 14 January 2017. http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm.
[951] The Directive on Security of Network and Information Systems (NIS Directive), Digital Single Market. 28 July 2016. Date of Access: 14 January 2017. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive.

laws while exchanging information on the education of cybercrime investigators, digital forensics, and the conduct of cybercrime investigations.[952]

On 14 November, 2016, experts from the EU Co-ordinating Office for Palestinian Police Support provided training to Palestinian lawyers in order to enhance their capacities in dealing with cyber crimes and to strengthen Palestine's legal system.[953]

On 25 November 2016, officials from the EU and the North Atlantic Treaty Organization (NATO) met to propose further advancements in cooperation regarding cyber defence including proposals for cooperation in information exchange and combatting cyber-attacks, and building on their earlier Technical Arrangement on Cyber Defense.[954]

On 2 December 2016, representatives from the EU joined NATO along with other states such as Algeria, Finland, Japan, Austria, Switzerland, and Sweden in NATO's annual Cyber Coalition Exercise in Estonia. More than 700 cyber defenders including legal experts, military officers, academics, and governmental officials gathered to train in combatting cyber-attacks by rapidly sharing information about cyber incidents and coordinating their defense tactics effectively.[955]

On 16 December 2016, the EU's cyber partnership with the US was further strengthened during the third meeting of the EU-US Cyber Dialogue in Brussels, during which both parties reaffirmed their support for the continuation of the United Nations Group of Governmental Experts by confirming that the existing principles of international law apply to the conduct of state behavior in cyberspace and that states should commit to following norms of responsible state behaviour.[956] Both parties also supported confidence building measures, promoted human rights, affirmed support for the Convention on Cybercrime, and agreed to coordinate their efforts in cyber resilience.[957]

The EU has acknowledged the application of international law in cyberspace through its global and domestic dialogue, promoted responsible state behaviour through its interstate partnerships, and taken confidence building measures in enhancing cyberspace stability through data protection and holding data processors accountable. As such, the EU has been given a score of +1.

Analyst: Fariha Ahmed

[952] Strategic Partnership Agreement between Canada, of the One Part, and the European Union and its Member States, of the Other Part, Global Affairs Canada (Ottawa) 14 November 2016. Date of Access: 19 January 2017. http://international.gc.ca/world-monde/international_relations-relations_internationales/can-eu_spa-aps_can-ue.aspx?lang=eng.
[953] EUPOL COPPS Delivers Training on Cyber Crimes for Palestinian Lawyers - EEAS - European Commission, European Union External Action Service (Brussels) 29 November 2016. Date of Access: 19 January 2017. https://eeas.europa.eu/headquarters/headquarters-homepage/16054/eupol-copps-delivers-training-cyber-crimes-palestinian-lawyers_bg.
[954] NATO and EU Press Ahead with Cooperation on Cyber Defence, Europa (Brussels) 25 November 2016. Date of Access: 19 January 2017. https://eeas.europa.eu/headquarters/headquarters-homepage/15917/nato-and-eu-press-ahead-with-cooperation-on-cyber-defence_en.
[955] NATO Holds Annual Cyber Exercise in Estonia, NATO (Brussels) 2 December 2016. Date of Access 19 January 2017. http://www.nato.int/cps/en/natohq/news_138674.htm.
[956] "Joint Elements" from the EU-U.S. Cyber Dialogue, U.S. Department of State (Washington DC) 23 December 2016. Date of Access: 18 January 2017. https://www.state.gov/r/pa/prs/ps/2016/12/265970.htm.
[957] "Joint Elements" from the EU-U.S. Cyber Dialogue, U.S. Department of State (Washington DC) 23 December 2016. Date of Access: 18 January 2017. https://www.state.gov/r/pa/prs/ps/2016/12/265970.htm.