The BGF-G7 Summit Initiative

Ise-Shima Norms

Governor Michael Dukakis

Professor Thomas Patterson

Nguyen Anh Tuan

Professor John Savage

Professor Derek Reveron

Allan Cytryn

Ryan Maness

Boston, May 9th 2016

Securing Cyberspace and the G7 Agenda*

The Boston Global Forum welcomes this opportunity to provide input to the agenda for the G7 Ise-Shima Summit. Global Economy and Trade, Development, and Quality Infrastructure Investment are three themes of this summit. Given the importance of the Internet in all three areas, we encourage you to address the following actions concerning cybersecurity at the summit. These actions have as their goal to raise the general level of security in cyberspace.

1. Encourage the global adoption of the 2015 G20 cybersecurity norms, which include the 2015 GGE norms by reference, as the Ise-Shima Norms.

2. Endorse private and public efforts to improve ethical Internet behavior. The UCLA Global Citizenship Education Program and the Boston Global Forum's Ethical Code of Conduct for Cyber Peace and Security are two such examples.

3. Engage vendors of cyberspace technology in the discussion of norms for responsible state behavior.

4. Establish domestic and international centers and mechanisms designed to reduce the risk of cyber conflict.

5. Encourage national cybersecurity experts to voluntarily publicize their best security practices.

6. Recognize that formulation of policy concerning cyberspace technologies requires the participation, on an equal footing, of respected academics and industry experts on the technologies in question.

The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).

These proposals stem from several developments.

First, over the last five years, small groups of governments have formulated international norms of state behavior, particularly for peacetime use. Negotiations have been held at the UN and many other forums. Now that a set of reasonable

*The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).

norms have been established it is appropriate to reach out to nations that have not participated in these discussions and encourage them to endorse them as well. In many cases, this will require some capacity development, which is encouraged by UN Resolution 70/237. The G7 nations can help increase confidence in computers and network technology by leading this effort, which could be called the Ise-Shima Challenge.

Second, global citizenship education has an important a role to play in building a sustainable peace and security in cyberspace. We encourage a significant effort in this regard.

Third, we observe that the success of many computer vendors requires that their customers have confidence in their products, which is undermined by unreported cyber vulnerabilities and by state launched weapons that result in mass events. Thus, some vendors, notably, Microsoft, have begun to formulate and promulgate norms of state behavior that are important from their point of view. States should take these nascent efforts seriously and engage these firms in norms formulation.

Fourth, given the large number of states that are developing cyber weapons, the risk of accidental or intentional cyber conflict is rising. All states should recognize this risk and work to mitigate it. Centers designed to reduce the risk of cyber conflict are needed in every country with offensive cyber capability. Operators in these centers must come to know each other so that they can properly assess national intentions during a cyber crisis. This issue has been highlighted in the latest 2015 GGE report.

The fifth recommendation on best practices is illustrated by a public talk given in January 2016 by Rob Joyce, head of NSA's Tailored Access Operations Department. He offered advice on cybersecurity

*The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).

measures to protect a computing facility from the type of penetration in which his department engages. This event was a remarkable example of the security services of a major nation, the US, offering constructive advice to others. Each G7 nation could assume the same responsibility for improving the security of cyberspace by offering such examples of best practices.

Finally, policy formulation concerning cyberspace can be very challenging. Unless technology experts are at the table with policymakers when such policy is formulated, errors are easily made that may lead to poorly formulated international norms or domestic legislation. Thus, it is essential that academic and technology experts be engaged and treated as co-equals with policymakers during this process.

The appendices that follow provide specific recommendations that have been developed by a variety of parties and are aligned with the above objectives.

The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).

Appendix A: The Ise-Shima Norms

The G7 nations should promote the development of social, legal and technological norms and agreements that will protect the information and communications infrastructures of the world's nations and their people. In doing so, these norms will promote the abilities of these technologies to fulfill their promise to enhance the lives of all. These actions follow successful precedents in many areas where international, national and private efforts have worked together to enable the world to realize the benefits of new technologies in order to maximize their benefit to all and to mitigate differences between nations and peoples.

I. The G7 nations should encourage adoption of norms set forth by the G20, the United Nations' Group of Government Experts (GGE), and the Boston Global Forum's Ethics Code of Conduct for Cybersecurity (ECCC).

1. Key G20 norms

·Nation-state conduct in cyber space should conform to international law and the UN charter**.**

·No country should conduct or support cyber-enabled intellectual property theft for commercial purposes.

2. Key GGE norms

·No country should intentionally damage the critical infrastructure of another state or impair infrastructure that serves the public and would undermine the human rights guaranteed by the U.N. Declaration.

·No country should act to impede the response of Computer Security Incident Response Teams (CSIRTs) to cyber incidents, nor should CSIRTs be used to create cyber incidents.

·Countries should cooperate with requests from other nations to investigate cybercrimes and mitigate malicious activity emanating from their territory.

3. Key ECCC norms

**The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).*

·Countries should not establish or support policies or actions harmful to cyberspace.
·Countries should not engage in the unlawful taking of the assets or confidential information of private individuals or organizations.

·Nations should not use cyberspace to wrongly damage the reputation of other nations, organizations, or individuals.

II. The G7 nations should engage hardware and software vendors in developing cyber norms, following the six guidelines in the Microsoft report, *"International Cyber Security Norms: Reducing Conflict in an Internet-Dependent World."*

1. Countries should not target information and communications technology (ICT) companies to insert vulnerabilities (backdoors) or take action that would undermine public trust in products and services.
2. Countries should have a clear principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors rather than stockpiling, buying, or selling them.
3. Countries should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.
4. Countries should commit to nonproliferation activities related to cyber weapons.
5. Countries should limit their engagement in cyber offensive operations to avoid creating a mass event.
6. Countries should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

III. The G7 nations should develop cyber risk reduction measures.

1. Create domestic threat reductions centers equipped with secure communications with other such national centers to mitigate risks before, during and after cyber-incidents.
2. Assess and improve the cyber security of national critical infrastructures.
3. Take steps to reduce the number of domestic compromised computers, particularly those that have been marshalled into botnets.
4. Improve domestic cybersecurity through advisory and legislative measures.

**The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).*

IV. The G7 nations should promote the development, identification, sharing and adoption of "best practices" in the cybersecurity area.

V. The G7 nations should support cyber security capacity building in developing countries.

1. Investments should be made in developing countries to secure their infrastructures as this is essential to securing the connected global infrastructure and preventing a widening gap in the capabilities of nations. In the interconnected world, these investments are essential to reducing costs resulting from cyber-crime and espionage and to increasing the confidence and trust of businesses to operate in developing countries.
2. Investments should be made and cooperation undertaken between developed and developing countries to re-envision methods of education and learning, utilizing the global information and telecommunication infrastructure to enhance the accessibility of suitable educational opportunities for people everywhere.

**The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).*

Appendix B

2015 GGE Norms

(Excerpt from UN A/70/174*)

The 2015 UN GGE committee consisted of experts from 20 representing Belarus, Brazil, China, Columbia, Egypt, Estonia, **France**, **Germany**, Ghana, Israel, **Japan**, Kenya, Malaysia, Mexico, Pakistan, the Republic of Korea, the Russian Federation, Spain, the **United Kingdom of Great Britain and Northern Ireland**, and the **United States of America**. The two G7 countries not represented are Canada and Italy.

"13. … (T) present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;
b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;
c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;
d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;
e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;
f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;
g) States should take appropriate measures to protect their critical infrastructure from ICT

**The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).*

* Retrieved from http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 on May 7, 2016.

threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;
i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;
j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;
k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

14. The Group observed that, while such measures may be essential to promote an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, in particular for developing countries, until they acquire adequate capacity."

In addition, the 2015 GGE encouraged states to implement confidence-building measures to include a) identification of domestic technical and policy points of contact "to address serious ICT incidents," b) risk reduction measures, c) sharing of general threat information, known technological vulnerabilities, and best security practices, and d) identification of critical domestic infrastructures and the legal, technical and assessment steps that nations have taken to protect them. This GGE also encouraged states to exchange law enforcement and cybersecurity personnel as well as to facilitate exchanges between academic and research institutions. The creation of national computer emergency response teams is also encouraged along with exchanges of personnel between such groups.

*The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).

Appendix C

G20 Cybersecurity Norms

Excerpt from the

G20 Leaders' Communiqué
Antalya Summit, 15-16 November 2015*

"A26. We are living in an age of Internet economy that brings both opportunities and challenges to global growth. We acknowledge that threats to the security of and in the use of ICTs, risk undermining our collective ability to use the Internet to bolster economic growth and development around the world.

1. We commit ourselves to bridge the digital divide. In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations.
2. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors.
3. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications. …
4. (W)e welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs. …
5. (We) commit ourselves to the view that all states should abide by norms of responsible state behaviour in the use of ICTs in accordance with UN resolution A/C.1/70/L.45. †
6. We are committed to help ensure an environment in which all actors are able to enjoy the benefits of secure use of ICTs. "

†G20 Members: Argentina, Australia, Brazil, **Canada**, China, **France**, **Germany**, India, Indonesia, **Italy**, **Japan**, Korea, Mexico, Russia, Saudi Arabia, South Africa, Turkey, **United Kingdom**, **United States**, and European Union. All G7 member states are members of the G20. Their names are in boldface.

**The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).*

* Retrieved from http://www.gpfi.org/sites/default/files/documents/G20-Antalya-Leaders-Summit-Communiqu--.pdf May 7, 2016.

† UN resolution A/C.1/70/L.45 incorporates the GGE Norms by reference.

*The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).

REFERENCES

Bloom, Les and John E. Savage. "On Cyber Peace." *The Atlantic Council,* August 2011, Accessed 3/4/2016 at
http://www.atlanticcouncil.org/images/files/publication_pdfs/403/080811_ACUS_OnCyberPeace.PDF

Boston Global Forum. "Ethics Code of Conduct for Cyber Peace and Security," December 12, 2015. Accessed 3/14, 2016 at

http://bostonglobalforum.org/2015/11/the-ethics-code-of-conduct-for-cyber-peace-and-security-eccc-version-1-0/

Nicholas, Paul. "Six Proposed Norms to Reduce Conflict in Cyberspace." 1/20/2015. Accessed 3/4/2016 at

http://blogs.microsoft.com/cybertrust/2015/01/20/six-proposed-norms/

Painter, Christopher. "G20: Growing International Consensus on Stability in Cyberspace." *State.gov,* 12/3/2015. Accessed 3/5/2016 at

https://blogs.state.gov/stories/2015/12/03/g20-growing-international-consensus-stability-cyberspace

Valeriano, Brandon and Ryan C. Maness. "The Coming Cyberpeace: The Normative Argument against Cyberwarfare." *Foreign Affairs.*5/13/2015. Accessed 3/3/2016.
https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace

The 2015 GGE norms are stated in paragraph 13 of "Developments in the field of information and telecommunications in the context of international security," UN Report A/70/174, July 22, 2015. Accessed 5/7/2016 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. The full set of GGE reports can be found at https://www.un.org/disarmament/topics/informationsecurity/

**The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).*

The 2015 G20 norms are stated in paragraph 26 of "G20 Leaders' Communiqué, Antalya Summit 2015", November 15-16, 2015. Accessed 5/7/2016 at http://www.gpfi.org/publications/g20-leaders-communiqu-antalya-summit-2015.

"The Ethics Code of Conduct for Cyber Peace and Security (ECCC)," Boston Global Forum, 9/3/2015. Accessed 5/7/2016 at http://bostonglobalforum.org/2015/11/the-ethics-code-of-conduct-for-cyber-peace-and-security-eccc-version-1-0/

*The lead author on this document was John Savage (Brown University) with contributions from Michael Dukakis (Boston Global Forum), Nguyen Anh Tuan (Boston Global Forum), Allan Cytryn (Risk Masters International.), Ryan Maness (Northeastern University), Derek Reveron (Naval War College), and Thomas Patterson (Harvard University).