EastWest INSTITUTE

Global Cyberspace Cooperation Summit VI

New York 2015

September 9 – 10, 2015

Breakthrough Group Working Papers

The EastWest Institute is proudly hosting the 2015 Global Cyberspace Cooperation Summit in New York City.

EWI's Global Cooperation in Cyberspace Initiative is convening policymakers, business leaders, technical experts and civil society with the objective to reduce conflict, crime and other disruptions in cyberspace and promote stability, innovation and inclusion.

This invitation-only meeting of international actors aims to coordinate and consolidate the initiative's progress, showcase results and promote collective action. The annual cyber summits provide a crucial forum for building international, private-public action to foster international cooperation in cyberspace. Breakthrough groups, aligned with the initiative's objectives of economic and political development, digital security and stability, and sound governance and management, carry the program forward.

Global Cyberspace Cooperation Summit VI
New York 2015

September 9-10, 2015

The Westin New York at Times Square
270 West 43rd Street
New York, NY 10036

Contents

Promoting Measures of Restraint in Cyber Armaments

Advocating Cyber Norms and Normative Behavior: Towards a Standing Forum

A Working Paper of the EastWest Institute Breakthrough Group
"Promoting Measures of Restraint in Cyber Armaments"

August 24, 2015

Summary

Events in 2015, especially agreement among the UN Group of Governmental Experts, hold out a new opportunity to lift the tempo of global advocacy of cyber norms and normative behavior. This opportunity has been framed by more than a decade of diverse and often disaggregated activism by states, businesses and civil society. The stakeholders have not arrived at consensus on some of the most serious issues affecting international security, but we have reached a new plateau that allows us to usefully reassess past efforts. The overarching lesson we can draw is that the classic institutions of international organization, either governmental or in the business sector—the current regime complex—benefited from the availability of activist NGOs to achieve this new plateau.

There is room to consider what more the NGO sector can do, how it can be better organized and directed towards the goal of bridging some of the remaining substantial divides on normative issues. We believe that this goal would be well served if committed stakeholders could deliver an enhanced focus to their efforts by establishing a new forum specifically for that purpose (or rejuvenating an existing one). This forum would have as its main goal the early take-up by states of new norms of mutual restraint or norms of common welfare in cyberspace. The characteristics of the ideal forum are laid out in the final section of the paper.

Attachment A offers a brief overview of the contribution of the EastWest Institute in this field, both by way of example (a possible model) and as a foundation for a decision by interested stakeholders (champions) to work with EastWest to develop the new forum.

This paper is accompanied by an additional paper providing a comparative analysis of emerging norms of state behavior related to the uses of information and communications technologies to commit internationally wrongful acts.

Discussion

Role of Neutral NGOs in Catalyzing Norm Development

Governments have long recognized the need to partner with business and civil society in framing new approaches to international norms and normative behavior in cyber space. The process has been developing over almost a decade, but has been slow to gather momentum and consistency. The international community now has a unique opportunity to ramp up its efforts. The character of this opportunity is revealed more fully by the coincidence of the following events:

- UN Group of Governmental Experts (GGE) agreement in 2015 on several priority areas for normative behavior;
- A commitment to continuing action by the Dutch government after the fourth summit in the London Process;
- General commitments in 2015 between Russia and China and China and the United States to normative behaviors toward each other in cyberspace (in very broad terms);
- Achievement of a critical mass in multi-stakeholder processes with universal appeal in NetMundial and the work of NGOs, especially by the EastWest Institute and ICT4Peace;
- Achievement of a critical mass in expert analysis of global approaches to norms and normative behavior through the work of organizations like Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn (the Manual) and corporations like Microsoft;
- Formation in 2014 of a Global Commission on Internet Governance.

In spite of this unprecedented opportunity, there is not yet a forum that carries the specific brief of promoting (rather than analyzing) the development of cyber norms and normative behavior in cyberspace or one with the requisite global buy-in. There is no forum which sees as its main mission the specific task of advocating (speeding up) norm development by states and other stakeholders on first order issues by promoting international agreements (regimes of practice, habits of cooperation, confidence building) on second order issues.

Figure 1 shows a representation of the existing "regime complex" governing cyberspace norm development, monitoring and observance developed by Joseph Nye.[1]

Figure 1: Nye's Regime Complex

Nye concludes that we are unlikely to see a "single overarching regime for cyberspace any time soon."[2] He talks correctly of a "good deal of fragmentation" and says it "is likely to persist." He observed that "Different sub-issues are likely to develop at different rates, with some progressing and some regressing in the dimensions of depth, breadth and compliance." Nye demonstrated this by identifying quite different areas of norm development for cyber activities (such as war, espionage, human rights, privacy, content control and standards) and characterized the current state of regime in these areas by four aspects (depth, breadth, fabric and compliance).[3] He cites Keohane and Victor, who describe the field of climate change policy development, as "actually many different cooperation problems, implying different tasks and structures."[4] They concluded that collaboration outcomes in each problem would sit variously on a scale of integration and

[1] Joseph S. Nye Jr, "The Regime Complex for Managing Global Cyber Activities", Belfer Center for Science and International Affairs, Harvard, 2014, p, 7, http://belfercenter.hks.harvard.edu/files/global-cyber-final-web.pdf.
[2] Nye op. cit. p.15.
[3] Nye op. cit. p. 8.
[4] Keohane, Robert O. and David G. Victor. 2011. "The Regime Complex for Climate Change", Perspectives on Politics, v. 9, issue 1, p. 8.

fragmentation in large part because of divergences in "power weighted" interests, the potential for gains or losses from linking sub-issues, and differences in how actors managed uncertainty.

These perspectives are helpful in explaining the institutional reality and also in turning actors toward more clarity about the nature of the problem and problem-solving pathways. But they are rooted in a traditional framing of international relations that privileges not just hierarchy but also states.

As an alternative, Figure 2 shows visual representation of where a proposed new forum might sit relative to key interest groups and the existing regime complex. The main target of action by this forum would still be states (as portrayed in the maroon arrow). One reason for this is that states are the actors most able to shape international security, including human security. (Security, broadly defined, remains the central concern of the EastWest Institute.) Another reason is that the main gap in policy mobilization is not only among states, but between states and the other newly influential private stakeholders.

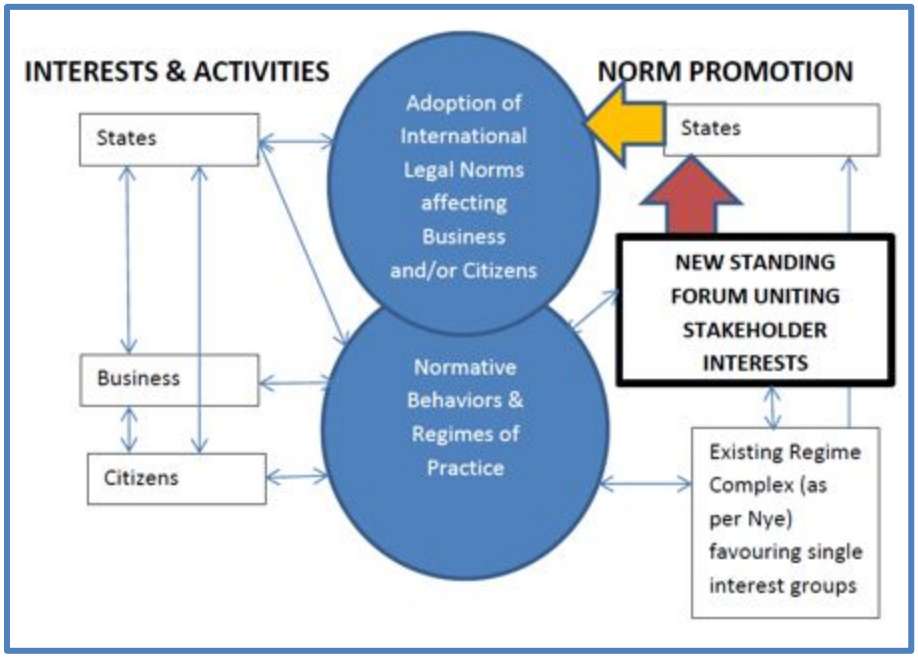


Figure 2: Proposed New Forum

Such a mechanism would capture consideration of three inter-linked dimensions:

- The need for urgency in regime or norm development in particular sub-fields. (Are agreements on cyber war, cyber espionage or content control more urgent than agreements on cybersecurity standards? Where can progress be made more rapidly?)
- The fragmentation of power as the result of two causes: deep intrusion of non-state actors into the material reality of what states and international organizations must manage, and the distributed moral authority of the information age.
- The dynamic nature of the political terrain that is emerging as a result of the rapidly expanding social evolution of cyberspace, including the transformation of pre-existing hierarchies and structuring, and the growth of global conversations about norms and regimes.

Whether we agree with the above characterizations or not, it is useful to be clear about assumptions about norms in cyberspace. As suggested by Keohane and Victor, even some of these assumptions may well be contested. Table 1 offers an indicative list of such assumptions that could be informing state action.

The character of the urgency of new normative behaviors is spelled out in many places, along with principles and recommendations. For example, apart from many excellent academic works,[5] in 2013, Microsoft issued a useful paper

[5] Michael Portnoy and Seymour Goodman (eds), *Global Initiatives to Secure Cyberspace: An Emerging Landscape*, Springer, New York: Springer 2009; M. Maybaum, A.-M. Osula, L. Lindström (eds), *Architectures in Cyberspace*, Tallinn: CCDCOE 2015; Nye, op. cit.; Michael

outlining "Five Principles for Shaping Cyber Security Norms". The work of the UN GGE forum is itself testimony to recognition of the need, even if its slow work over more than a decade belies a commitment to a shared sense of urgency.

ASSUMPTIONS ABOUT THE TERRAIN OF NORMS IN INTERNATIONAL LAW

1. Discussions are often confounded by loose usage of the term "norms" which has several meanings depending on the context (international legal norms, domestic legal norms, moral norms, political norms, professional norms, business norms, and so on).
2. An international legal norm can be one that is universally agreed (with universal application) or one limited to a group of consenting states (applying only to the consenting states).
3. New international legal norms with universal application usually take decades (if not a century or two) to develop and become accepted as norms.
4. Norms are often constituted by "regimes" (of practice) that subsequently become legal norms.
5. Normative behaviors (such as consultation, self-restraint and dispute resolution by peaceful means) can be adjuncts to or even substitutes for norms.
6. Practices unregulated by norms coexist with emerging norms, universally accepted norms and contested norms.
7. Politics, like diplomacy, is a contest over the right to dictate norms or at least have the upper hand in shaping norm development OR shaping an argument about how to interpret and implement existing norms.

ADDITIONAL ASSUMPTIONS ABOUT THE NORMATIVE TERRAIN OF CYBERSPACE

1. Cyberspace is ubiquitous and highly variegated: norms, laws and contested practices of cyberspace are ubiquitous and highly variegated.
2. Some examples: IPR law, trade law, investment law, labor law, human rights, state responsibility, diplomatic (sovereign) immunity, Law of the Sea, air and space, air traffic control, disaster relief, pandemic control, LOAC, private international law, extradition treaties, non-aggression treaties.
3. States are only one category of actor in cyberspace and they no longer have a monopoly on determining norms.
4. Ethical and political contest over the meaning of existing or emerging norms is severely magnified and exaggerated at all levels by netizen power and private sector power.

Table 1: Indicative List of Assumptions about the Normative Terrain of Cyberspace[6]

N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Conflict*, Cambridge: Cambridge University Press, 2013; Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms", Tallinn Paper No. 5, Special Expanded Issue, NATO CCDCOE, Tallinn, 2014; Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace", *American Foreign Policy Interests*, 36: 322-331, 2014; Ludovica Glorioso and Anna Maria Osula (eds), *1st Workshop on Ethics of Cyber Conflict: Proceedings*, CDC COE, Tallinn, 2014; "A Call to Cyber Norms: Discussions at the Harvard-MIT-University of Toronto Cyber Norms Workshops, 2011 and 2012", Belfer Center, Harvard University, 2015; Tim Maurer, "Cyber Norm Emergence at the United Nations", Belfer Center, Harvard University, Boston, 2011; Enneken Tikk-Ringas, "Developments in the Field of Information and Telecommunications in the Context of International Security: Work of UN First Committee 1998-2012", ICT4Peace, Geneva, 2012; Camino Kavanagh, Tim Maurer and Enneken Tikk –Ringas, "Baseline Review: ICT-Related Processes & Events: Implications for International and Regional Security (2011-2013)", ICT4Peace, Geneva, 2014; Abdul Paliwala, "Netizenship, security and freedom", *International Review of Law, Computers and Technology*, 2013, vol. 27, Nos. 1-2, 104-123.

[6] See Greg Austin, "China's Position on Norms in Cyber Space", CCDCOE Cycon Paper, 2015, in publication as part of an edited volume edited by Anna Maria Osula.

Formulas for Success in Civil Society Norm Entrepreneurship

One of the best sets of guidance for NGOs involved in norm entrepreneurship has been framed by Dr. Moreton Bergsmo, who was prominent in the establishment and work of the International Criminal Court (ICC). In 2004, he gave a detailed assessment of setting up the ICC to an NGO roundtable in Brussels. Having noted how most international lawyers and politicians laughed at the idea of an ICC when it was first mooted, he identified the underlying normative foundations for the court, such as the Nuremberg principles. He also noted the advances in international criminal jurisdiction made during the 1990s, beginning with the UN Security Council decision to set up a Committee of Experts and followed by other measures, both within the International Law Commission and in practice (especially Security Council acquiescence in the use by a Special Representative of the Secretary General in two different missions of war crimes authority). He noted the effect of the creation of other conflict specific tribunals (ICTY, Sierra Leone and Cambodia) on acceptance of the idea of an ICC.

Most importantly, for the purpose of significant reform in the international legal framework, Dr. Bergsmo identified six essential factors:

1. NGO mobilization and unity.
2. Competent, well-informed specialists and lawyers in those NGOs.
3. Sufficient transparency in the multilateral process for NGOs to be effective.
4. A few principled states to protect the integrity of the idea throughout the reform deliberations.
5. Adequate great power acceptance to provide hard political legitimacy.
6. Established NGO "laboratories" to show the feasibility of the project.

Dr. Morten Bergsmo noted the difference between "codification" as the concrete manifestation of existing state practice or norms of custom accepted as law, and "codification" designed to be a vehicle of reform or change with a view to "positivising" a norm or ideal rather than a specific rule.

In the same roundtable, participants agreed that a similar set of ingredients had contributed to the success of the campaign to ban land mines, resulting in the Ottawa Treaty; and in the campaign for international regulation of the arms trade, especially small arms, which resulted over a slightly longer period in the UN Arms Trade Treaty.

Prioritizing Norms in any New Forum: Changing Needs, Showcasing Collaboration

We must address the question of which areas of cyberspace are the highest priority for norm entrepreneurship. For an organization such as the EastWest Institute, we aim to address the most intractable issues of international security where we can act (reframe, convene, mobilize) and where we see unmet needs in areas that engage the multi-stakeholder character of security in cyberspace.

Our work on cyberspace issues, like this Breakthrough Group on Promoting Measures of Restraint in Cyber Armaments, is premised on the view that we should continue to proceed on dual tracks: work with all of the stakeholders to forge new international and universal regimes to address important selected challenges in a workable and visibly short time frame; and use that process and its successes to promote the principle of normative behavior across the geopolitical divides to achieve concrete and measurable outcomes. Any new forum would need to learn from the EastWest experience that the appetite in the stakeholder community for (and need for) particular lines of work will change over time.

By mid-2015, a long list of potential areas has emerged, with various levels of complexity, and diverse opinion, including those identified by:

- UN Group of Governmental Experts in 2015.
- The Foreign Minister of the Netherlands at the Global Cyberspace Conference in The Hague in 2015.
- Microsoft's paper on norms in 2014, titled *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*.
- Tallinn Manual 2013 (commissioned in 2009).
- Russia, China and like-minded states in the proposed Code of Conduct tabled at the UN in 2011.
- The UK Foreign Minister at the Munich Security Conference in February 2011.

- Work of the EastWest Institute, IEEE, CCDCOE in Tallinn, the Harvard Belfer Center, Centre for Strategic and International Studies, China Institute for Contemporary International Relations, ICT4Peace, the UN Institute for Disarmament Research, (and many other researchers and organizations) mostly beginning in 2009 or later.
- The ITU's High Level Expert Group on Cyber Security in 2009.
- The World Federation of Scientists in 2008.
- The World Summit on Information Society between 2002 and 2005.
- The UN General Assembly in annual resolutions beginning in 1998.

Characteristics of the Forum

The essential characteristics would be:

- One of two main goals—the early take-up by states of new norms (or normative behaviors) of mutual restraint.
- A second main goal—the early take-up by all stakeholders of new norms (or normative behaviors) of common welfare in cyber space.
- Operates on issues where there is large scale intermingling among governmental, business and/or citizen interests.
- Includes at least three well-placed states, three well-placed corporations and three well-placed civil society organizations as its enduring partners and champions.
- Enjoys the broad and consistent support of other leading states (e.g. those in the GGE and their peers) and related international actors (ICANN and ITU), as well as their active participation in its work.
- Maintains geopolitical neutrality even as it seeks to pressure states toward earlier agreement on new norms than might be possible if states were left to their own devices.
- Takes on an annual review and analytical function (stock-take) regarding stakeholder behavior in cyberspace and suggested norms.
- Commits to more vigorous and effective programs of advocacy around the general goal of normative behavior, more than any NGO has been able to deliver so far.
- Mobilizes critical analysis by scholars and stakeholders from around the world.
- Secures commitments to move faster and produce outcomes that help catalyze existing forums.
- Represents multi-stakeholder interests better than existing forums.
- Establishes early claims to be an entirely appropriate adjunct to state action and an effective adjunct to state action.
- Profiles new approaches, especially from states, businesses or citizens outside the dominant discourses of the West that have not yet gained traction or been treated appropriately in existing forums.
- Secures a nimble organizational structure but a permanent staff adequate to the task.
- Sustains funding of at least $2 million per year, preferably closer to $4 million.

How Would the Forum Evolve?

The EastWest Breakthrough Group (BG) would champion the creation of the new forum, and the BG may itself transition to be the backbone of the new forum. But the focus of this BG over six months would be to debate the above considerations and make recommendations that at least several leading states and other key stakeholders can endorse for the formal establishment and funding of the new forum. The work of the BG would culminate in a report documenting both evolution of the concept and buy-in from champions among states and leading corporations. Depending on how it evolves, the new forum might be called one of the following:

- Forum for Normative Practices in Cyberspace (perhaps based in The Hague).
- Network for Regimes of Practice in Cyberspace (with hubs in major cyber powers).
- Global Cyberspace Cooperation Initiative (based in EastWest).

There are benefits and downsides to each of the three models. The absolute minimum requirement we can levy on the new forum is that it be staffed, funded and supported to achieve early take-up by key stakeholder groups of new normative behaviors and to continue to advocate effectively for that.

Attachment A: EastWest Institute as a Model or Foundation

Since 2006, the EastWest Institute has been involved in some way in international regime formation for cyberspace. The work has varied in that period, from focus on breakthroughs in individual areas of international cyber policy (e-signatures, spam, priority communications, supply chain integrity) to promotion of stability in inter-state relations on big issues of war, peace and diplomacy involving Russia, China and the United States. We always saw the two broad dimensions as linked, with progress on more concrete business and community issues contributing to the building of confidence and trust among states. To this end, EastWest has consistently partnered with leading governments, businesses and civil society groups in our cyberspace work. It is our experience, documented extensively elsewhere, and confirmed by the sustained engagement of many parties in a range of non-governmental efforts, that much needs be done, more effectively and more rapidly, to bring stability, order and security to many aspects of cyberspace activity while preserving and promoting its economic and social benefits. Table A-1 provides a list of our policy papers in support of this work.

- *The Cybersecurity Agenda: Mobilizing for International Action* (2010)
- *Global Cyber Deterrence* (2010)
- *Rights and Responsibilities in Cyber Space: Balancing the Need for Security and Liberty* (2010)
- *Russia, the United States and Cyber Diplomacy: Opening the Doors* (2010)
- *Protecting the Digital Economy* (2011) (2010 Summit Report)
- *Working Towards Rules for Governing Cyber Conflict: Rendering the Geneva and Hague Conventions in Cyberspace* (2011) (US-Russia Working Group)
- *Fighting Spam to Build Trust* (2011)
- *Critical Terminology Foundations* (2011) (US-Russia working group)
- *Mobilizing for International Action* (2011) (Summit Report)
- *Priority International Communications* (2012) (US-China working group)
- *Cyber Détente between the United States and China* (2012)
- *Frank Communication and Sensible Cooperation to Stem Harmful Hacking* (2013) (US-China working group)
- *Critical Terminology Foundations 2* (2014) (US-Russia working group)
- *A Measure of Restraint in Cyberspace: Reducing Risk to Civil Nuclear Assets* (2014)
- *Resetting the System: Why highly secure computing should be the priority of cyber security policies* (2014)

Table A-1: List of EastWest Policy Reports and Discussion Papers

The work agenda for any new forum should probably remain shaped by the original principle guiding the work of the EastWest: the most influence on stakeholders can be achieved through completion of showcase agendas for changes in specific sub-fields in a reasonably short time, while maintaining a broad dialogue with stakeholders globally for legitimacy, feedback and guidance. Figure A-1 sketches the policy space that EastWest occupies.

Emerging Norms of State Behavior Related to the Uses of Information and Communications Technologies to Commit Internationally Wrongful Acts: A Comparative Snapshot

A Working Paper of the EastWest Institute Breakthrough Group
"Promoting Measures of Restraint in Cyber Armaments"

August 24, 2015

A variety of documents have been developed by governments, multilateral and intergovernmental organizations, and corporations that propose norms of State behavior designed to mitigate or reduce certain malicious activity in cyberspace. We have chosen five reference documents here for comparative analysis:

- Shanghai Cooperation Organization Code of Conduct, January 2015 (SCO)[1]
- U.S. Policy, from remarks by U.S. Secretary of State John Kerry in Seoul, May 2015 (USG)[2]
- United Nations Group of Governmental Experts on Information Security, August 2015 (UNGGE)[3]
- NATO Tallinn Manual, 2013 (Tallinn)[4]
- Microsoft Norms paper, *International Cybersecurity Norms: Reducing Conflict in an Internet-Dependent World*, December 2014 (MSFT)[5]

These documents cover a broad variety of areas related to cyberspace policy. We have focused on the portions of each document that propose a norm of behavior directed at reducing certain malicious activity in cyberspace. These common emerging norms fall into five general categories:

I. Basic principles ensuring the security and stability of global cyberspace.
II. The responsibility of States to avoid and to prevent certain types of cyber attacks launched from their territories.
III. The responsibility of States to enhance the security of information and systems within their territories.
IV. The duty of States to cooperate with each other to mitigate certain types of cyber incidents.
V. Restraint in the development and use of cyber weapons in peace time.

In each category, at least two of the reference documents propose one or more norms of State behavior. Below we show the text and briefly analyze the areas of agreement and disagreement. Table 1, at the end of this document, presents a snapshot of all the norms discussed.

[1] "International code of conduct for information security," January 9, 2015, http://www.un.org/ga/search/view_doc.asp?symbol=A/69/723. The members of the Shanghai Cooperation Organization are: People's Republic of China, Kazakhstan, Kyrgyz Republic, Russia, Tajikistan, and Uzbekistan.
[2] "An Open and Secure Internet: We Must Have Both," May 18, 2015, http://www.State.gov/secretary/remarks/2015/05/242553.htm.
[3] "Developments in the Field of Information and Telecommunications in the Context of International Security," A/70/172, http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174. The participants in the 2014-2015 UN GGE for Information Security are: Belarus, Brazil, China, Colombia, Egypt, Estonia, France, Germany, Ghana, Israel, Japan, Kenya, Malaysia, Mexico, Pakistan, Russian Federation, Spain, United Kingdom and United States.
[4] "Tallinn Manual on the International Law Applicable to Cyber Warfare", 2013, https://ccdcoe.org/tallinn-manual.html. The Manual does not represent the views of NATO or its sponsoring nations. In particular, it is not meant to reflect the NATO doctrine.
[5] "Proposed Cybersecurity Norms to Reduce Conflict in an Internet-dependent World," December 14, 2014, https://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/.

I. Basic principles ensuring the security and stability of global cyberspace.

From SCO, two:

(1) Comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity, and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries.

(7) To recognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive, and impart information, taking into account that [international law][6] attaches to that right special duties and responsibilities....

From USG, one:

Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.

From UNGGE, two:

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 agreed to be harmful or that may pose threats to international peace and security.

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions A/HRC.RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/Res/69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the fright to freedom of expression.

Analysis: The norms here recognize the kinds of balance that is often found in international agreements between the rights of States to defend themselves against internal and external threats and the need for action to maintain international peace and security. For example, the U.S. Statement, "Acts of aggression are not permissible," is balanced by an assertion of the "right to respond." There are, of course, differing views on such language, whether the response is in cyberspace or through diplomatic or other means. Some would say it enhances peace and stability by creating a deterrent, while others would impute a destabilizing threat.

II. The responsibility of States to avoid and to prevent certain types of cyber attacks launched from their territories.

From the SCO, two:

(2) Not to use information and communications technologies and information and communications networks to carry out activities, which run counter to the task of maintaining international peace and security.

(3) Not to use ICTs and ICT networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability.

[6] The full text reads, ". . . the International Covenant on Civil and Political Rights (article 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (ordre public), or of public health or morals."

From the USG, three:

1. No country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure.

3. No country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain.

4. Every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.

From the UNGGE, two:

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

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.

From Tallinn, one:

5. A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.

Analysis: The USG, Tallinn, and GGE positions calling on States to "mitigate malicious cyber activity emanating from its soil," "not knowingly allow their territory to be used for internationally wrongful acts," and "not knowingly allow the cyber infrastructure located in its territory … to be used for acts that adversely and unlawfully affect other States" suggest that if a State becomes aware that some third party—whether an individual, group of individuals, another State, or, perhaps an apparatus of the State itself—is using the ICT infrastructure within its territory for internationally wrongful acts, that State has a responsibility to try to stop the activity. In the non-cyber world, States have long been able to arrest or extradite other individuals suspected of committing piracy, slavery or genocide.

III. The responsibility of States to enhance the security of information and systems within their territories.

From the SCO, two:

(6) To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage.

(5) To endeavor to ensure the supply chain security of information and communications technology goods and services…

From UNGGE, three:

g. States should take appropriate measures to protect their critical infrastructure from ICT threats.

i. States should take reasonable steps to ensure the integrity of the supply chain, so 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, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

From Tallinn, two:

1. A State may exercise control over cyber infrastructure and activities within its sovereign territory.

2. Without prejudice to international obligations, a State may exercise its jurisdiction: (a) over persons engaged in cyber activities on its territory; (b) over cyber infrastructure located on its territory; and, (c) extraterritorially, in accordance with international law.

From MSFT, two:

1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in [commercial] products and services.

2. States should have a clear principle-based policy for handling product and services vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.

Analysis: Secure infrastructure depends significantly on secure technology. Microsoft's first proposed norm, regarding the insertion by States of vulnerabilities in commercial ICT products and services companies, is unsurprisingly stronger than the government-led GGE recommendation that States take reasonable steps to maintain the integrity of the supply. Similarly, a key aspect missing from the government-centric GGE effort would be an additional norm limiting government action to undermine international security standards efforts to benefit their own interests.

This aspect of the norm will come under increasing scrutiny as the debate about "ubiquitous encryption," and law enforcement access to communications content under legal process, moves into the global policy environment.[7] The Kerry speech (USG) does not address the responsibility for securing systems within national boundaries as an international norm, perhaps because it is seen as a domestic matter. However it is certainly true that the U.S. government is taking steps to secure U.S. critical infrastructure.[8] The same can be said of most of the GGE participating governments.

IV. The duty of States to cooperate with each other to mitigate certain types of cyber incidents.

From the SCO, one:

(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds.

From the USG, one:

5. Every country should do what it can to help States that are victimized by a cyberattack.

From the UNGGE, two:

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 another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty.

[7] For two different U.S. perspectives, see, "Why the fear over ubiquitous data encryption is overblown," Washington Post, July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html; and, "When Phone Encryption Blocks Justice," August 11, 2015, http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html?_r=0.

[8] See, *inter alia,* Executive Order No. 13636, "Improving Critical Infrastructure Cybersecurity;" Presidential Policy Directive (PPD)-21, "Critical Infrastructure Security and Resilience;" both are from February 12, 2013. More recently, see, "Cybersecurity Enhancement Act of 2014," P.L. 113-274, December 18, 2014.

b. In case of ICT incidents, States should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.

From MSFT: one:

6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.

Analysis: Increasingly in cyber incidents, information on combating threats is not only, or even primarily, in the hands of a national government response team. In the hours and days after an incident, multiple actors—from other countries—often contribute to identifying and then solving the issue. Today, information sharing often begins as an ad hoc collaboration, particularly during a crisis that aligns disparate sectors and even competitors toward a unified, collective response. For example, in 2008, the Conficker Working Group came together to share information and develop a response to the Conficker worm which had infected millions of computers around the world. Similarly, in the recent attacks against Sony Entertainment, corporate and government teams from several countries worked together to mitigate the effects of the attacks. Participants in these responses were willing to share information because there was a mutual benefit to be gained from the collective response, not least the trust developed between the responders, notably between government responders and private sector participants.

The various norms proposed in this "mutual assistance" section have the potential to enhance and further drive existing models of collaboration. Effective incident response efforts depend both on the maturity of public and private sector response capabilities as well as trusted relationships to enable information-sharing between them. Norms can help foster trust and build confidence, but they are not in themselves sufficient. Ongoing operational, functional, pragmatic cooperation and enhanced transparency around policies and response structures are vital elements in this context. Cooperation can become more challenging "curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds" (SCO-4). Differing standards across cultures can make for disagreements at the margins about what content falls under free speech, however offensive it may be. Continued dialogue will increase understanding here, but differences will remain.[9]

V. Restraint in the development and use of cyber weapons in peace time.

From the SCO, one:

(2) Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security.

From USG, two:

Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.

2. No country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.

From the UNGGE, one:

k. States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity.

From Tallinn, one:

9. A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.

[9] The work of the Internet Jurisdiction Project (www.internetjurisdiction.net) is instructive and useful in this regard.

From MSFT, three:

3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable.

4. States should commit to nonproliferation activities related to cyber weapons.

5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.

Analysis: Perhaps five years ago there was hope that cyberspace could remain "fundamentally a civilian space — a neighborhood, a library, a marketplace, a school yard, a workshop — and a new, exciting age in human experience, exploration and development."[10] Today, with dozens of nations building offensive cyber capabilities, such a hope seems naïve. A non-weaponized cyberspace is unlikely. In the non-cyber world, the Proliferation Security Initiative[11] calls upon participating countries to interdict WMD related materials, especially if that State's ports or infrastructure is being used to facilitate the transport and proliferation of WMD materials. In the text supporting its proposed norm 4 (nonproliferation), Microsoft calls on States to collaborate "with international partners and, to the extent practicable, private industry," noting that such collaboration would "help reduce the possibility that cyber weapons could be used by non-State actors."

Preliminary Conclusions

1. There is considerable superficial convergence in norms, both in the general principles (Category I) and in particular areas such as mutual assistance (Category IV). This is a promising development, suggesting that where there is emerging agreement there is the possibility of more immediate and practical progress.
2. Serious areas of disagreement also remain, notable amongst them are differing understandings as to the appropriate limits of State sovereignty, stemming in substantial part from cultural, political, and military factors.
3. Relatedly, the asymmetric distribution of cyber capabilities across States affects preferences and emphases on norms. In this guise, one might imagine progress will be faster should there be a more equal distribution of necessary capabilities among actors.
4. Such equalization could be viewed as contrary to the emerging nonproliferation norm, with the potential destabilizing effect of increasing the militarization of cyberspace. Equalization, without significant progress on measures of restraint, is thus inadvisable. The lack of attention to such measures in most of the documents reviewed is disappointing, and it undermines the commitment to reducing tension and promoting stability. In addition to reducing the spread of cyber weapons, measures of restraint in action would provide additional avenues to enhancing peace in cyberspace. Such measures could include: non-aggression or no-first-use pledges; identifying assets that should not be attacked, particularly in peace time; and stronger work to help legitimate actors protect themselves and each other (thus raising the costs to attackers).

The EastWest Institute Breakthrough Group on "Promoting Measures of Restraint in Cyber Armaments" looks forward to the discussion of this working paper and these conclusions in New York September 9-10.

[10] See, "Op-Ed: A Civil Perspective on Cybersecurity," Jane Holl Lute and Bruce McConnell, *Wired,* February 14, 2011, http://www.wired.com/2011/02/dhs-op-ed/.
[11] See, http://www.psi-online.info/. Some have suggested that something like the PSI might work in cyber.

Table 1: Comparative Study of Emerging Norms of State Behavior Related to the Uses of Information and Communications Technologies to Commit Internationally Wrongful Acts

Generic Norm Type	Source of Detailed Norm	
	SCO	Kerry Seoul Speech, May 18, 2015
I. Basic principles ensuring the security and stability of global cyberspace	(1) Comply with the Charter of the United Nations and universally recognized norms governing international relations that enshrine, inter alia, respect for the sovereignty, territorial integrity, and political independence of all States, respect for human rights and fundamental freedoms and respect for the diversity of history, culture and social systems of all countries. (7) To recognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive, and impart information, taking into account that [international law] attaches to that right special duties and responsibilities....[complete text in body of paper]	Acts of aggression are not permissible. And countries that are hurt by an attack have a right to respond in ways that are appropriate, proportional, and that minimize harm to innocent parties.
II. The responsibility of States to avoid and to prevent certain types of cyber attacks launched from their territories	(2) Not to use information and communications technologies and information and communications networks to carry out activities which run counter to the task of maintaining international peace and security. (3) Not to use ICTs and networks to interfere in the internal affairs of other States or with the aim of undermining their political, economic and social stability.	1. No country should conduct or knowingly support online activity that intentionally damages or impedes the use of another country's critical infrastructure. 3. No country should conduct or support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information for commercial gain. 4. Every country should mitigate malicious cyber activity emanating from its soil, and they should do so in a transparent, accountable and cooperative way.
III. The responsibility of States to enhance the security of information and systems within their territories	(6) To reaffirm the rights and responsibilities of all States, in accordance with the relevant norms and rules, regarding legal protection of their information space and critical information infrastructure against damage resulting from threats, interference, attack and sabotage. (5) To endeavor to ensure the supply chain security of information and communications technology goods and services	
IV. The duty of States to cooperate with each other to mitigate certain types of cyber incidents	(4) To cooperate in combating criminal and terrorist activities that use information and communications technologies and information and communications networks, and in curbing the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds.	5. Every country should do what it can to help states that are victimized by a cyberattack.
V. Restraint in the development and use of cyber weapons in peace time		2. No country should seek either to prevent emergency teams from responding to a cybersecurity incident, or allow its own teams to cause harm.

Source of Detailed Norm		
UN GGE on Information Security, Aug. 2015, Sec. 13	Tallinn Manual on the International Law Applicable to Cyber Warfare	Microsoft Paper: "International Cybersecurity Norms," Dec. 2014
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 agreed to be harmful or that may pose threats to international peace and security. e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions A/HRC.RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/Res/69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the fright to freedom of expression.		
c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. 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.	5. A State shall not knowingly allow the cyber infrastructure located in its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States.	
g. States should take appropriate measures to protect their critical infrastructure from ICT threats. i. States should take reasonable steps to ensure the integrity of the supply chain, so 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, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.	1. A State may exercise control over cyber infrastructure and activities within its sovereign territory. 2. Without prejudice to international obligations, a State may exercise its jurisdiction: (a) over persons engaged in cyber activities on its territory; (b) over cyber infrastructure located on its territory; and, (c) extraterritorially, in accordance with international law.	1. States should not target ICT companies to insert vulnerabilities (backdoors) or take actions that would otherwise undermine public trust in [commercial] products and services. 2. States should have a clear principle-based policy for handling product and services vulnerabilities that reflects a strong mandate to report them to vendors rather than to stockpile, buy, sell, or exploit them.
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 another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty. b. In case of ICT incidents, States should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences.		6. States should assist private sector efforts to detect, contain, respond to, and recover from events in cyberspace.
k. States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams. A State should not use authorized emergency response teams to engage in malicious international activity.	9. A State injured by an internationally wrongful act may resort to proportionate countermeasures, including cyber countermeasures, against the responsible State.	3. States should exercise restraint in developing cyber weapons and should ensure that any which are developed are limited, precise, and not reusable. 4. States should commit to nonproliferation activities related to cyber weapons. 5. States should limit their engagement in cyber offensive operations to avoid creating a mass event.

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

United Nations General Assembly, July 2015

Summary

Information and communications technologies (ICTs) provide immense opportunities and continue to grow in importance for the international community. However, there are disturbing trends that create risks to international peace and security. Effective cooperation among States is essential to reduce those risks.

The 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security examined existing and potential threats arising from the use of ICTs by States and considered actions to address them, including norms, rules, principles and confidence-building measures. In addition, the Group examined how international law applies to the use of ICTs by States. Building on the work of previous Groups, the present Group made important progress in those areas.

The present report significantly expands the discussion of norms. The Group recommended that States cooperate to prevent harmful ICT practices and should not knowingly allow their territory to be used for internationally wrongful acts using ICT. It called for the increased exchange of information and assistance to prosecute terrorist and criminal use of ICTs. In doing so, the Group emphasized that States should guarantee full respect for human rights, including privacy and freedom of expression.

One important recommendation was that a State should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure. States should also take appropriate measures to protect their critical infrastructure from ICT threats. States should not harm the information systems of the authorized emergency response teams of another State or use those teams to engage in malicious international activity. States should encourage the responsible reporting of ICT vulnerabilities and take reasonable steps to ensure the integrity of the supply chain and prevent the proliferation of malicious ICT tools, techniques or harmful hidden functions.

Confidence-building measures increase cooperation and transparency and reduce the risk of conflict. The Group identified a number of voluntary confidence-building measures to increase transparency and suggested that States consider additional ones to strengthen cooperation. The Group called for regular dialogue with broad participation under the auspices of the United Nations and through bilateral, regional and multilateral forums. While States have a primary responsibility to maintain a secure and peaceful ICT environment, international cooperation would benefit from the appropriate participation of the private sector, academia and civil society.

Capacity-building is essential for cooperation and confidence-building. The 2013 report of the Group (see A/68/98) called for the international community to assist in improving the security of critical ICT infrastructure, help to develop technical skills and advise on appropriate legislation, strategies and regulation. The present Group reiterated those conclusions and emphasized that all States can learn from each other about threats and effective responses to them.

The Group emphasized the importance of international law, the Charter of the United Nations and the principle of sovereignty as the basis for increased security in the use of ICTs by States. While recognizing the need for further study, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group also noted the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction.

In its thinking on future work, the Group proposed that the General Assembly consider convening a new Group of Governmental Experts in 2016.

The Group asks Member States to actively consider their recommendations and assess how they might be taken up for further development and implementation.

Foreword by the Secretary-General

Few technologies have been as powerful as information and communications technologies (ICTs) in reshaping economies, societies and international relations. Cyberspace touches every aspect of our lives. The benefits are enormous, but these do not come without risk. Making cyberspace stable and secure can be achieved only through international cooperation, and the foundation of this cooperation must be international law and the principles of the Charter of the United Nations.

The present report contains recommendations developed by governmental experts from 20 States to address existing and emerging threats from uses of ICTs, by States and non-State actors alike, that may jeopardize international peace and security. The experts have built on consensus reports issued in 2010 and 2013, and offer ideas on norm-setting, confidence-building, capacity-building and the application of international law.

Among the complex issues that have emerged is the growing malicious use of ICTs by extremists, terrorists and organized criminal groups. The present report provides suggestions that can help to address this worrisome trend and contribute to the formulation of my forthcoming plan of action on preventing violent extremism.

All States have a stake in making cyberspace more secure. Our efforts in this realm must uphold the global commitment to foster an open, safe and peaceful Internet. In that spirit, I commend the present report to the General Assembly and to a wide global audience as a crucial contribution to the vital effort to secure the ICT environment.

Letter of transmittal

26 June 2015

I have the honour to submit herewith the report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. The Group was established in 2014 pursuant to paragraph 4 of General Assembly resolution 68/243 on developments in the field of information and telecommunications in the context of international security. As Chair of the Group, I am pleased to inform you that consensus was reached on the report.

In its resolution, the General Assembly requested that a group of governmental experts be established in 2014, on the basis of equitable geographical distribution, to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States, as well as the concepts aimed at strengthening the security of global information and telecommunications systems. The Group was also asked to take into account the assessments and recommendations of a previous Group (see A/68/98). The Secretary-General was requested to submit a report on the results of the study to the Assembly at its seventieth session.

In accordance with the terms of the resolution, experts were appointed from 20 States: Belarus, Brazil, China, Colombia, 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 list of experts is contained in the annex.

The Group had a comprehensive, in-depth exchange of views on developments in the field of information and telecommunications in the context of international

security. It met in four sessions: the first from 21 to 25 July 2014 at United Nations Headquarters, the second from 12 to 16 January 2014 in Geneva and the third from 13 to 17 April 2015 and the fourth from 22 to 26 June 2015, both at United Nations Headquarters.

The Group would like to thank the experts who served as facilitators in the discussions on the draft report: Florence Mangin (France), Katherine Getao (Kenya), Ausaf Ali (Pakistan), Ricardo Mor (Spain) and Olivia Preston (United Kingdom).

The Group wishes to express its appreciation for the contribution of the United Nations Institute for Disarmament Research, which served as a consultant to the Group and was represented by James Lewis and Kerstin Vignard. The Group also wishes to express its appreciation to Ewen Buchanan of the United Nations Office for Disarmament Affairs, who served as Secretary of the Group, and to other Secretariat officials who assisted the Group.

(*Signed*) Carlos Luís Dantas Coutinho **Perez**
Chair of the Group

I. Introduction

1. Pursuant to General Assembly resolution 68/243 on developments in the field of information and telecommunications in the context of international security, the Secretary-General, on the basis of equitable geographical distribution, established a group of governmental experts to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies (ICTs) in conflicts and how international law applies to the use of ICTs by States, as well as relevant international concepts aimed at strengthening the security of global information and telecommunications systems.

2. An open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security. The present report reflects the recommendations of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and builds upon the work of previous Groups (see A/65/201 and A/68/98). The Group examined relevant international concepts and possible cooperative measures pertinent to its mandate. It reaffirmed that it is in the interest of all States to promote the use of ICTs for peaceful purposes and to prevent conflict arising from their use.

II. Existing and emerging threats

3. ICTs provide immense opportunities for social and economic development and continue to grow in importance for the international community. There are, however, disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security.

4. A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely.

5. The most harmful attacks using ICTs include those targeted against the critical infrastructure and associated information systems of a State. The risk of harmful ICT attacks against critical infrastructure is both real and serious.

6. The use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.

7. The diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict and the possibility of harm to their citizens, property and economy.

8. Different levels of capacity for ICT security among States can increase vulnerability in an interconnected world.

III. Norms, rules and principles for the responsible behaviour of States

9. The ICT environment offers both opportunities and challenges to the international community in determining how norms, rules and principles can apply to State conduct of ICT-related activities. One objective is to identify further voluntary, non-binding norms for responsible State behaviour and to strengthen common understandings to increase stability and security in the global ICT environment.

10. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.

11. Previous reports of the Group reflected an emerging consensus on responsible State behaviour in the security and use of ICTs derived from existing international norms and commitments. The task before the present Group was to continue to study, with a view to promoting common understandings, norms of responsible State behaviour, determine where existing norms may be formulated for application to the ICT environment, encourage greater acceptance of norms and identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed.

12. The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security (see A/69/723).

13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the 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 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.

15. Given the unique attributes of ICTs, additional norms could be developed over time.

IV. Confidence-building measures

16. Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability. In their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H). To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:

(a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;

(b) The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;

(c) Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;

(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:

(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;

(ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;

(iii) The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;

(iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.

17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to:

(a) Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;

(b) Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;

(c) Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;

(d) Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;

(e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

18. The Group reiterates that, given the pace of ICT development and the scope of the threat, there is a need to enhance common understandings and intensify cooperation. In this regard, the Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums and other international organizations.

V. International cooperation and assistance in ICT security and capacity-building

19. States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment, but some States may lack sufficient capacity to protect their ICT networks. A lack of capacity can make the citizens and critical infrastructure of a State vulnerable or make it an unwitting haven for malicious actors. International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use. Providing assistance to build capacity in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action. The Group agreed that capacity-building measures should seek to promote the use of ICTs for peaceful purposes.

20. The Group endorsed the recommendations on capacity-building in the 2010 and 2013 reports. The 2010 report recommended that States identify measures to support capacity-building in less developed countries. The 2013 report called upon the international community to work together in providing assistance to: improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use. The present Group also emphasized that capacity-building involves more than a transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats.

21. Continuing the work begun through previous United Nations resolutions and reports, including General Assembly resolution 64/211, entitled “Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures”, States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance:

(a) Assist in strengthening cooperative mechanisms with national computer emergency response teams and other authorized bodies;

(b) Provide assistance and training to developing countries to improve security in the use of ICTs, including critical infrastructure, and exchange legal and administrative best practices;

(c) Assist in providing access to technologies deemed essential for ICT security;

(d) Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;

(e) Facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders;

(f) Develop strategies for sustainability in ICT security capacity-building efforts;

(g) Prioritize ICT security awareness and capacity-building in national plans and budgets, and assign it appropriate weight in development and assistance planning. This could include ICT security awareness programmes designed to educate and inform institutions and individual citizens. Such programmes could be carried out in conjunction with efforts by international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations;

(h) Encourage further work in capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs.

22. The development of regional approaches to capacity-building would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach.

23. In the interest of ICT security capacity-building, States may consider forming bilateral and multilateral cooperation initiatives that would build on established partnership relations. Such initiatives would help to improve the environment for effective mutual assistance between States in their response to ICT incidents and could be further developed by competent international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations.

VI. How international law applies to the use of ICTs

24. The 2013 report stated that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Pursuant to its mandate, the present Group considered how international law applies to the use of ICTs by States.

25. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.

26. In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the

purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.

27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

28. Building on the work of the previous Groups, and guided by the Charter and the mandate contained in General Assembly resolution 68/243, the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States:

(a) States have jurisdiction over the ICT infrastructure located within their territory;

(b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;

(c) Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group recognized the need for further study on this matter;

(d) The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;

(e) States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;

(f) States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated.

29. The Group noted that common understandings on how international law applies to State use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment.

VII. Conclusions and recommendations for future work

30. There has been significant progress in recognizing the risks to international peace and security from the malicious use of ICTs. Recognizing that ICTs can be a driving force in accelerating progress towards development, and consistent with the need to preserve global connectivity and the free and secure flow of information, the Group considered it useful to identify possible measures for future work, which include, but are not limited to, the following:

(a) Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels;

(b) Increased cooperation at regional and multilateral levels to foster common understandings on the potential risks to international peace and security posed by the malicious use of ICTs and on the security of ICT-enabled critical infrastructure.

31. While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.

32. Areas where further research and study could be useful include concepts relevant to State use of ICTs. The United Nations Institute for Disarmament Research, which serves all Member States, is one such entity that could be requested to undertake relevant studies, as could other relevant think tanks and research organizations.

33. The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour. Further work could consider initiatives for international dialogue and exchange on ICT security issues. These efforts should not duplicate ongoing work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights and Internet governance.

34. The Group noted the importance of the consideration by the General Assembly of the convening of a new Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security in 2016 to continue to study, with a view to promoting common understandings on existing and potential threats in the sphere of information security and possible cooperative measures to address them, as well as how international law applies to the use of ICTs by States, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building.

35. The Group acknowledges the valuable efforts in ICT security made by international organizations and regional groups. Work among States on security in the use of ICTs should take these efforts into account, and Member States should, when appropriate, encourage the establishment of new bilateral, regional and multilateral platforms for dialogue, consultation and capacity-building.

36. The Group recommends that Member States give active consideration to the recommendations contained in the present report on how to help to build an open, secure, stable, accessible and peaceful ICT environment and assess how they might be taken up for further development and implementation.

Annex

List of members of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

Belarus
Aliaksandr Chasnouski (third and fourth sessions)
Deputy Head of the Department of International Security and Arms Control, Ministry of Foreign Affairs

Ambassador Vladimir N. Gerasimovich (first session)
Head of the Department of International Security and Arms Control, Ministry of Foreign Affairs

Ivan Grinevich (second session)
Counsellor at the Permanent Mission of Belarus to the United Nations in Geneva

Brazil
Carlos Luís Dantas Coutinho Perez
Minister, Chief of Staff of the Vice-Minister for Political Affairs, Ministry of External Relations

China
Haitao Wu (third and fourth sessions)
Coordinator for Cyber Affairs of Ministry of Foreign Affairs

Cong Fu (first and second sessions)
Coordinator for Cyber Affairs of Ministry of Foreign Affairs

Colombia
Jorge Fernando Bejarno
Director of Standards and Architecture of Information Technology, Ministry of Information Communications Technology

Egypt
Sameh Aboul-Enein
Ambassador, Deputy Assistant Foreign Minister for Disarmament, International Security and Peaceful Uses of Nuclear Energy, Ministry of Foreign Affairs

Amr Aljowaily (third session)
Minister, Permanent Mission of Egypt to the United Nations

Estonia
Marina Kaljurand
Undersecretary and Legal Adviser, Ministry of Foreign Affairs

France
Florence Mangin
Ambassador, Coordinator for Cyber Security, Ministry of Foreign Affairs

Leonard Rolland (first session)
Department of Strategic Affairs, Security and Disarmament, Ministry of Foreign Affairs

Germany
Karsten Geier
Head, Cyber Policy Coordination Staff, Federal Foreign Office

Ghana
Mark-Oliver Kevor
Member of the Board of Directors of the National Communications Authority

Israel
Iddo Moed
Cyber Security Coordinator, Ministry of Foreign Affairs

Japan
Takashi Okada (third and fourth sessions)
Ambassador in charge of United Nations Affairs and Ambassador in charge of Cyber Policy, Deputy Director General, Foreign Policy Bureau, Ministry of Foreign Affairs

Akira Kono (second session)
Ambassador in charge of United Nations Affairs and Ambassador in charge of Cyber Policy, Deputy Director General, Foreign Policy Bureau, Ministry of Foreign Affairs

Takao Imafuku (first session)
Senior Negotiator on International Security Affairs, Foreign Policy Bureau, Ministry of Foreign Affairs

Kenya

Katherine Getao
ICT Secretary, Ministry of Information, Communications and Technology

Malaysia
Nur Hayuna Abd Karim (fourth session)
Principal Assistant Secretary, Cyber and Space Security Division, National Security Council

Md Shah Nuri bin Md Zain (first, second and third sessions)
Undersecretary, Cyber and Space Security Division, National Security Council

Mexico
Edgar Zurita
Attaché to the United States of America and Canada, Mexican National Security Commission — Federal Police

Pakistan
Ausaf Ali (first, second and fourth sessions)
Director General, Technical Branch, Strategic Plans Division, Joint Staff Headquarters

Khalil Hashmi (third session)
Minister, Permanent Mission of Pakistan to the United Nations

Republic of Korea
Chul Lee (second and fourth sessions)
Director, International Security Division, Ministry of Foreign Affairs

Hyuncheol Jang (first and third sessions)
Counsellor, Embassy of the Republic of Korea to the Kingdom of Belgium and the European Union

Russian Federation
Andrey V. Krutskikh
Special Representative of the President of the Russian Federation for International Cooperation in Information Security, Ambassador-at-large

Spain
Ricardo Mor (fourth session)
Ambassador-at-large for Cybersecurity, Ministry of Foreign Affairs and Cooperation

Alicia Moral (first, second and third sessions)
Ambassador-at-large for Cybersecurity, Ministry of Foreign Affairs and Cooperation

United Kingdom of Great Britain and Northern Ireland
Olivia Preston
Assistant Director, Office of Cyber Security and Information Assurance, Cabinet Office

United States of America
Michele G. Markoff
Deputy Coordinator for Cyber Issues, Office of the Coordinator for Cyber Affairs,

Modernizing International Procedures against Cyber-enabled Crimes

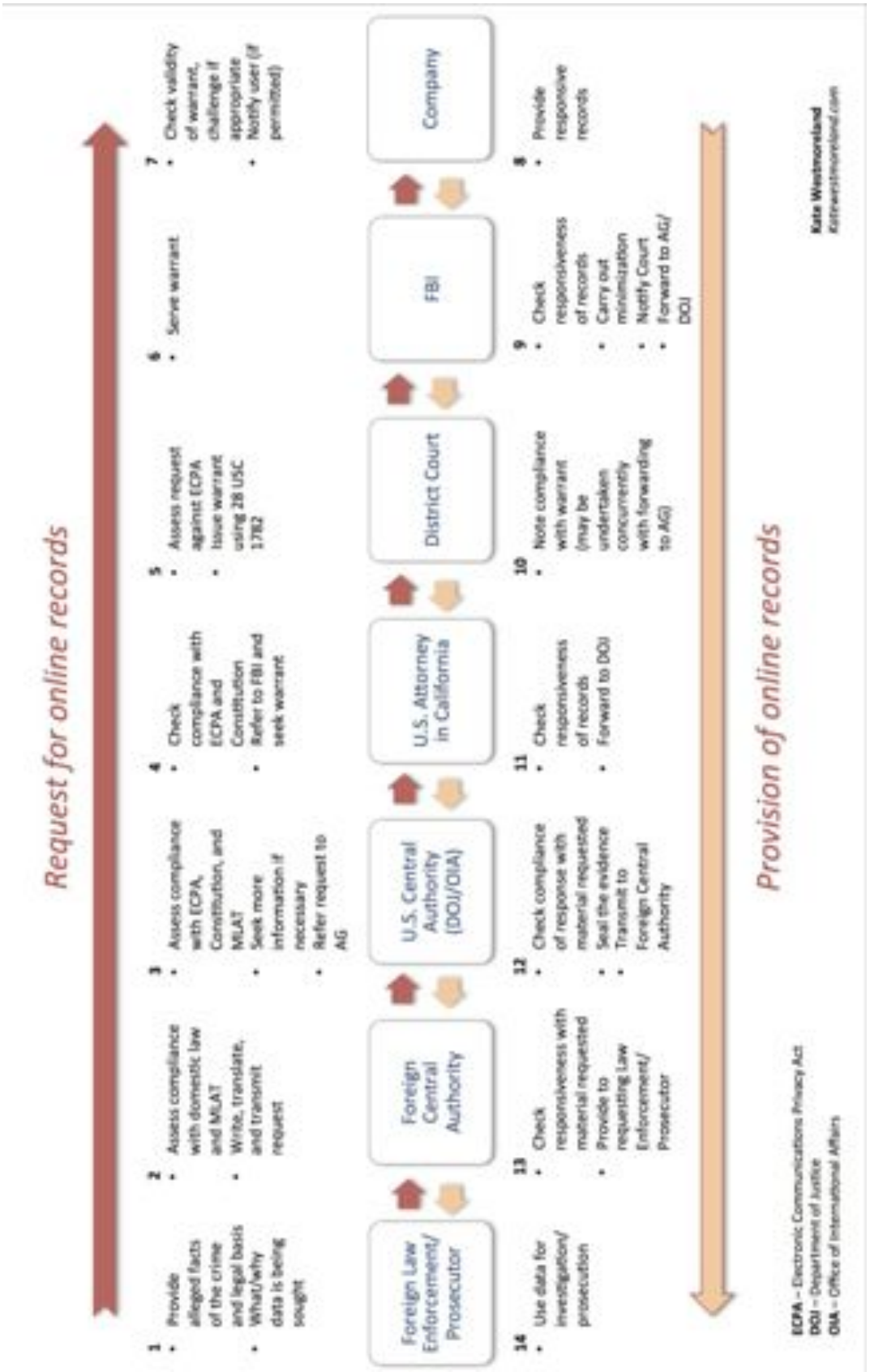
About the EastWest Institute Breakthrough Group on "Modernizing International Procedures against Cyber-enabled Crimes"

This Breakthrough Group is working to combat cyber crime and cyber criminals by improving cooperation between law enforcement and the private sector on a global basis. The group is initially focusing on (i) increasing the transparency of corporate response policies; and (ii) developing a standard format for information requests under mutual legal assistance procedures. This workbook includes two documents relevant to this work.

The first document, *Model Corporate Notice: Law Enforcement Assistance Request Policy*, responds to the challenge that law enforcement entities have in understanding and connecting with private companies who may be in possession of data relevant to an ongoing criminal investigation. While some companies have posted policies that guide law enforcement in these matters, most have not. The posted policies that do exist vary widely in level of detail and understandability. At the meeting on September 9, the Breakthrough Group will seek feedback on the draft policy notice and begin planning how to promote its use among key private sector actors.

The second document relates to an automated authoring tool for requests for assistance under Mutual Law Enforcement Assistance (MLA) procedures. The tool has been developed by the United Nations Office on Drugs and Crime (UNODC), and is being revised again at a meeting in mid-October. In September, the Breakthrough Group will discuss the tool and provide feedback to participants who are working directly with the UNODC authoring group. In particular, the BG will examine the extent to which modifications to the tool would make it more relevant and effective for use in cyber crime investigations.

Process for Obtaining User Data from California under a Mutual Legal Assistance Treaty (MLAT)



Model Corporate Notice:
Law Enforcement Assistance Request Policy

A Working Paper of the EastWest Institute Breakthrough Group
"Modernizing International Procedures against Cyber-enabled Crimes"

August 24, 2015

Purpose

These guidelines are for law enforcement officials seeking records from CompanyName. For private requests, including requests from civil litigants and criminal defendants, visit: www.____.___. Users seeking information on their own accounts should visit: www.____.___.

Policy

CompanyName assists law enforcement agencies in their investigations while protecting subscriber/user privacy consistent with our terms of service and as required by law and applicable privacy policies.

CompanyName's primary goal is to provide timely and accurate responses to all law enforcement and legal requests. Unless otherwise required, CompanyName's goal is to provide a response within ___ business days of each request.

International Requests

We respond to legal requests from jurisdictions outside of the United States where we have a good faith belief that the response is required by law in that jurisdiction, affects users in that jurisdiction, and is consistent with internationally recognized standards. All such legal requests must be completely in English. A Mutual Legal Assistance Treaty request or Letter Rogatory may be required to compel disclosure of information.

On a voluntary basis, we may provide user data in response to valid legal process from non-U.S. government agencies, if those requests are consistent with international norms, U.S. law, CompanyName's policies and the law of the requesting country.

Information We Collect and Maintain

In the course of conducting our business, we collect and maintain certain information and records about our subscribers and their activities, as detailed in our terms of use/privacy policies. For a detailed description of the information we collect and maintain, visit: www.____.___.

Records Access and Preservation

We will search for and disclose data that is specified with particularity in an appropriate form of legal process and which we are reasonably able to locate and retrieve. We normally retain [types of information] for a period of ___ days, consistent with legal requirements. We will take steps to preserve account records in connection with official criminal investigations for ___ days pending our receipt of formal legal process, unless applicable law provides otherwise.

Notification

Our policy is to notify people who use our service of requests for their information prior to disclosure unless we are prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when

notice would be counterproductive. We will provide delayed notice upon expiration of a specific non-disclosure period in a court order and where we have a good faith belief that exceptional circumstances no longer exist and we are not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other appropriate process establishing that notice is prohibited. If your data request draws attention to an ongoing violation of our terms of use, we will take action to prevent further abuse, including actions that may notify the user that we are aware of their misconduct.

Child Safety

We prioritize and report all apparent instances of child exploitation appearing on our site from anywhere in the world to the National Center for Missing and Exploited Children (NCMEC). NCMEC coordinates with the International Center for Missing and Exploited Children and law enforcement authorities from around the world. If a request relates to a child exploitation or safety matter, please specify those circumstances (and include relevant NCMEC report identifiers) in the request to ensure that we are able to address these matters expeditiously and effectively.

Emergency Requests

We are permitted to release [types of information] on an expedited basis in situations where there is an immediate danger of death, serious bodily injury or harm to a child. Proper legal process must be submitted after the emergency has subsided.

Cost Reimbursement

We may seek reimbursement for costs we incur responding to requests. We do not charge for responses to legal process served by a government entity involving with child exploitation. Where time allows, our policy is to discuss reimbursement with the requesting party before we incur any costs.

Submission of Requests

Online: Law enforcement officials may submit and track requests by requesting access at the link: www.____.____. Please note that a government-issued email address is required to access this link.

Mail:

Phone: For further information, call: NNN-NNN-NNNN.

UNODC Mutual Legal Assistance Request Writer Tool

The UNODC has created a tool to assist law enforcement officials in the preparation of mutual legal assistance (MLA) requests. Step by step, the MLA Tool guides the casework practitioner through the request process for each type of mutual assistance, using a series of templates. Before progressing from one screen to the next, the drafter is prompted if essential information has been omitted. Finally, the tool consolidates all data entered and automatically generates a correct, complete and effective request for final editing and signature.

The tool:

- Requires virtually no prior knowledge or experience with drafting mutual legal assistance requests.
- Helps to avoid incomplete requests for mutual legal assistance and therefore minimizes the risk of delay or refusal.
- Adjusts easily to any country's substantive and procedural law.
- Enables the user to retrieve key information on treaties and national legislation.
- Features an integrated case-management tracking system for incoming and outgoing requests.

Link to UNODC's Mutual Legal Assistance Request Writer Tool: https://www.unodc.org/mla/en/index.html

You can download a demo at: https://www.unodc.org/mla/demonstration-of-the-mla-tool.html

(Special thanks to Philipp Amann, European Cybercrime Centre, for bringing this to our attention!)

Frequently Asked Questions About the MLA Tool

Why should I use the MLA Tool?

- The MLA Tool guides criminal justice practitioners to draft requests for mutual legal assistance using a series of templates
- The MLA Tool covers all standard MLA types of assistance derived from international best practice. You can easily add others as they evolve.
- The MLA Tool works for your entire criminal law casework.
- The MLA Tool was developed, tested and accepted by practitioners for practitioners.

Can this MLA Tool be adapted to national requirements?

Yes, and you don't need to be a computer expert to do it. You can easily adjust the MLA Tool at any time to your domestic law and practice by adding or editing the template data through the Main Menu.

How much does the MLA Tool tell me about other country's legal systems and requirements?

- The MLA Tool gives you details and full contact particulars of where to send your request in other States.
- The MLA Tool also includes links to useful legislation sites of other countries. You can supplement these through your own web-searches.
- The MLA Tool does not spell-out the legal system requirements of other countries, because it is not yet possible to gather and maintain accurate, up-to-date information globally.
- There are a number of national and regional authorities that provide succinct summaries and manuals. These resources complement the MLA Tool.

How much does the MLA Tool cost?

- The MLA Tool is *free of charge.*
- And it helps reduce your costs - effective requests are generated with least possible time and cost and the authors are trained in the process.

How secure is the MLA Tool?

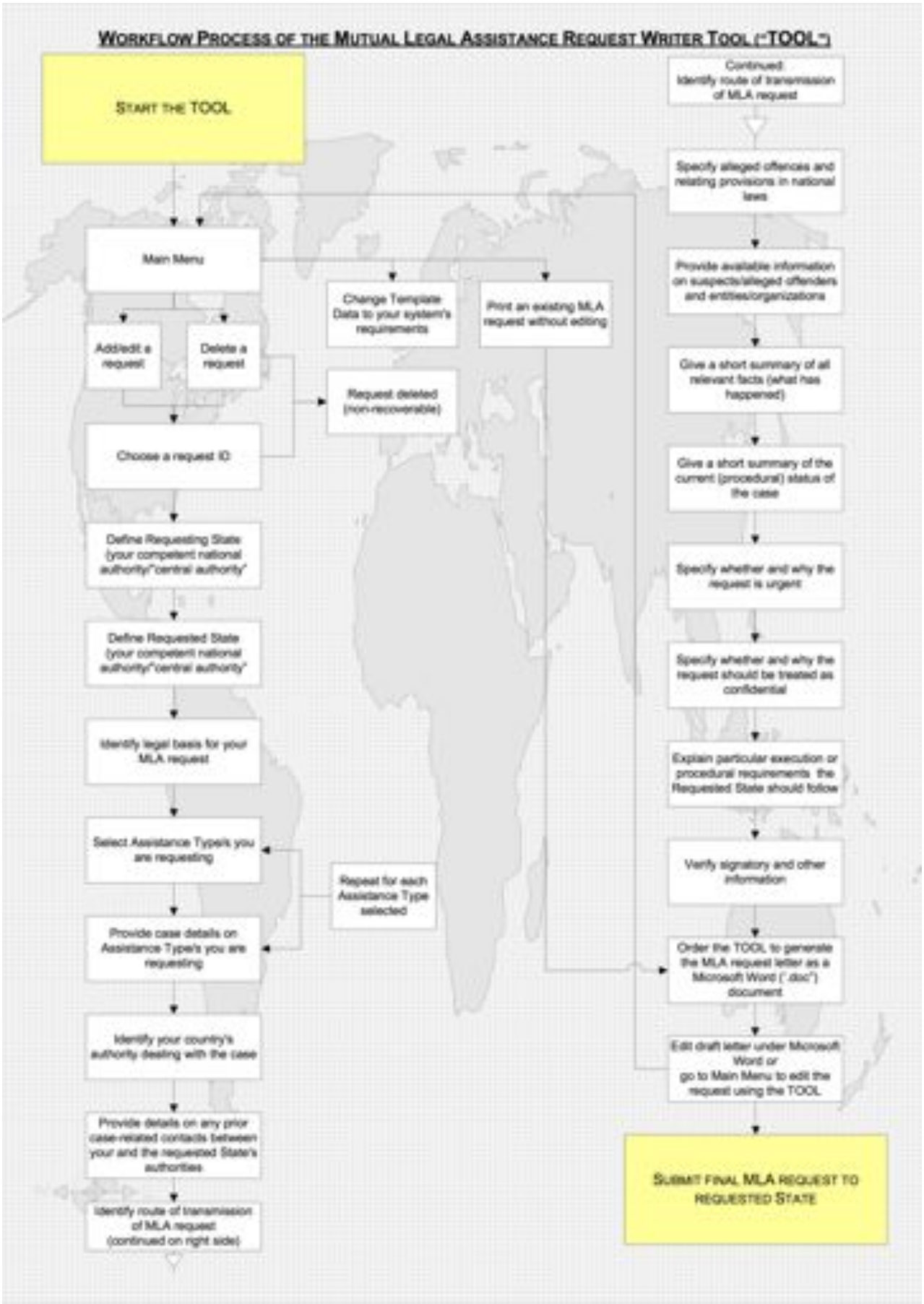
The MLA Tool is as secure as your computer system (either a server/network or individual PC/hard drive). Computer security is your responsibility. Possible security threats are computer-viruses as well as access by unauthorized persons. The MLA Tool is not encrypted. Please note that encryption programmes might influence the formatting of some of the underlying programming in the MLA Tool.

Is the MLA Tool available in all languages?

- You can currently download the English, French, Spanish, Russian, Bosnian, Croatian, Montenegrin, Portuguese and Serbian versions. The Portuguese version, was initiated and financed by the Ministries of Justice of Brazil and Portugal and the Montenegrin version was initiated and financed by the OSCE Mission in Montenegro.
- Albanian, Arabic and Macedonian language versions are underway.
- Please note that it is possible to translate the MLA Tool into other main languages. If you wish to initiate such translation, UNODC's Organized Crime and Criminal Justice Section can assist you.

Can the MLA Tool automatically translate requests into other languages?

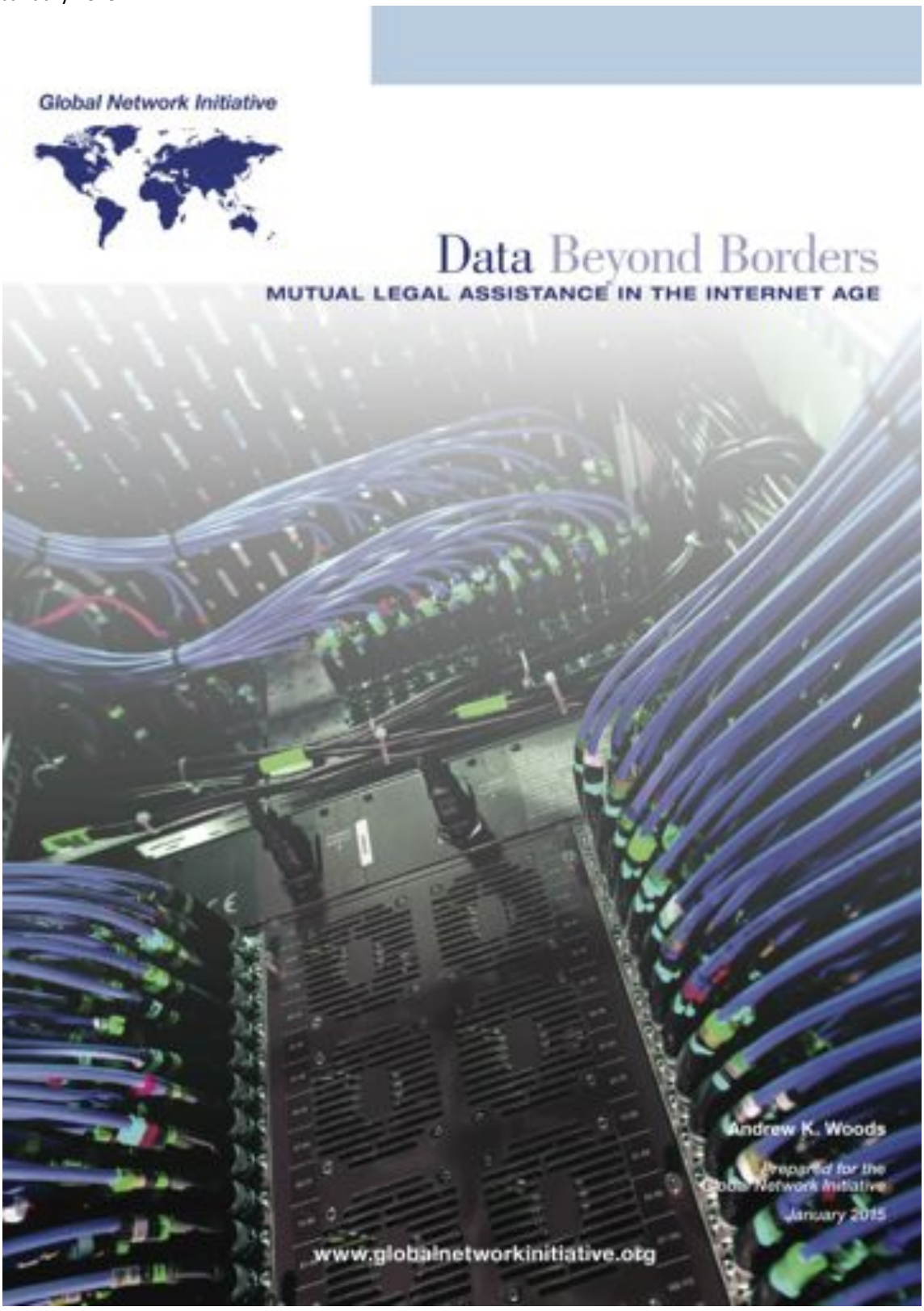
No, the MLA Tool itself does not translate the request, but you can always translate the final MLA request document to other languages, as required. Each MLA Tool version only creates MLA requests in one language, using your inputs, which you have made in this language. For example, the Spanish MLA Tool version only creates Spanish MLA requests, and all inputs must be made in Spanish. To find out language requirements, check the relevant MLA treaties, or if necessary liaise with the requested State on what languages are accepted by them for your MLA request. Write the MLA request with the Tool either in your own language or one you are proficient in. Submit the final MLA request in the language you have created it in, together with a certified translation into the language specified by the requested State. Other language versions of the Tool can also be downloaded to help your translators with technical terms in the language required by the Requested State. In case the MLA Tool is not yet available in your language nor one that you are proficient in, write the request in your own language, following the proposed structure identified in the Manual, and have the final document translated into the required language.


WORKFLOW PROCESS OF THE MUTUAL LEGAL ASSISTANCE REQUEST WRITER TOOL ("TOOL")
START THE TOOL
Main Menu
Add/edit a request
Delete a request
Choose a request ID
Define Requesting State (your competent national authority"central authority"
Define Requested State (your competent national authority"central authority"
Identify legal basis for your MLA request
Select Assistance Type/s you are requesting
Provide case details on Assistance Type/s you are requesting
Identify your country's authority dealing with the case
Provide details on any prior case-related contacts between your and the requested State's authorities
Identify route of transmission of MLA request (continued on right side)
Change Template Data to your system's requirements
Print an existing MLA request without editing
Request deleted (non-recoverable)
Repeat for each Assistance Type selected
Continued: Identify route of transmission of MLA request
Specify alleged offences and relating provisions in national laws
Provide available information on suspects/alleged offenders and entities/organizations
Give a short summary of all relevant facts (what has happened)
Give a short summary of the current (procedural) status of the case
Specify whether and why the request is urgent
Specify whether and why the request should be treated as confidential
Explain particular execution or procedural requirements the Requested State should follow
Verify signatory and other information
Order the TOOL to generate the MLA request letter as a Microsoft Word (".doc") document
Edit draft letter under Microsoft Word or go to Main Menu to edit the request using the TOOL
SUBMIT FINAL MLA REQUEST TO REQUESTED STATE

Excerpt

Data Beyond Borders: Mutual Legal Assistance in the Internet Age

January 2015



EXECUTIVE SUMMARY

The global nature of today's Internet services presents a unique challenge to international law enforcement cooperation. On a daily basis, law enforcement agents in one country seek access to data that is beyond their jurisdictional reach; as one industry analyst put it, there has been, "an internationalization of evidence." In order to gain lawful access to data that is subject to another state's jurisdiction, law enforcement agents must request mutual legal assistance (MLA) from the country that can legally compel the data's disclosure. But the MLA regime has not been updated to manage the enormous rise of requests for MLA. This report reviews existing MLA law and policy and proposes a number of reforms.

This report draws from dozens of wide-ranging conversations with a diverse set of stakeholders, including law enforcement agents from around the world, global Internet and telecommunications companies, and civil society groups large and small. Out of these conversations, five key principles have emerged—principles that ought to drive MLA reform for the twenty-first century. First, a country's request for MLA must be justified, and the level of assistance the country enjoys should be proportional to the country's interest in the data. Second, reforms must encourage respect for human rights: protecting user privacy, narrowly tailoring how much data is requested and transmitted, and so on. Third, reforms must increase the transparency of the existing MLA regime. Fourth, reforms must significantly increase the efficiency of the existing regime. Fifth and finally, reforms must be scalable in order to manage the coming wave of government requests for MLA.

There are a number of specific MLA reforms to be implemented. Three significant and urgent reforms are as follows:

1. **Electronic MLA:** Countries must develop an electronic system for submitting, managing, and responding to MLA requests. This is a huge undertaking, and should begin with the United States, the country that is most often on the receiving end of MLA requests. The system could begin on a voluntary basis with incentives for countries to opt-in.

2. **MLA Education:** Government officials—particularly law enforcement agents—must be trained to craft narrowly tailored and legitimate requests for MLA. Better understanding about what sorts of data can be lawfully accessed through the MLA regime and what data can be accessed outside the regime could have a significant impact on the number of the requests for MLA.

3. **MLA Staffing:** The number of MLA requests is rising quickly. Until the process becomes more streamlined—and even after it has been maximally streamlined—additional staff will be necessary to review, track, and process incoming MLA requests. More MLA staff are also needed to evaluate and process outgoing requests for MLA. As a result, MLA staffing should be an urgent priority for every country in the world.

MLA reform will not be easy. Because countries have diverging incentives depending on whether they tend to make requests for MLA or receive requests for MLA, and because they do not all agree on the appropriate grounds for providing MLA, reforms may be most promising among like-minded states. Because the MLA regime is essentially bilateral, the central challenge to reform is strong leadership and political will. Fortunately, there are compelling arguments for why all states should take a leadership role in MLA reform. First, when the MLA regime does not function swiftly and fairly, governments resort to other tactics such as demanding data localization, attempting to apply their laws extraterritorially, or worse, such as persecuting technology companies and their users. Second, all states benefit from a more robust system of MLA. Even states that do not typically seek MLA will likely need to do so – and quickly – when their citizens begin using an Internet service that for whatever reason lies beyond the state's jurisdictional reach.

Strengthening Critical Infrastructure Resilience and Preparedness

A Community-Based Platform for Critical Infrastructure Cyber Resilience

A Working Paper of the EastWest Institute Breakthrough Group
"Strengthening Critical Infrastructure Resilience and Preparedness"

August 24, 2015

Summary

The growing digitization and interconnection of society, and in particular critical infrastructures, increases the risk of accidental or deliberate cyber disruptions. Significant attention is being given to reducing cyber-related risk in many countries. However, a lack of awareness of the importance of cyber risk management, particularly among the owners and operators of small- and medium-sized critical infrastructure facilities and organizations, creates unacceptable risks across national economies.

The EWI Breakthrough Group on "Strengthening Critical Infrastructure Resilience and Preparedness (CIRP)" proposes to develop an action-oriented, interactive, community-based platform where critical infrastructure owners and operators can share stories related to cyber incidents and increase their awareness of cyber risk management.

The platform will feature two elements:

- Stories and case studies of critical infrastructure cyber risks and responses, contributed by community members.
- Risk assessment and management questions and techniques.

Definition

For the purposes of this work, the term "critical infrastructure" means the assets, systems and networks so vital that their incapacitation or destruction would have a debilitating national or regional effect on security, the economy, public health, safety or quality of life.

Stories and Case Studies

We included the following story as an initial example for discussion:

A report[1] of the German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik (BSI)) released just before Christmas indicated that hackers had attacked an unnamed steel mill in Germany. They were able to compromise the control system and disable a blast furnace's ability to be properly shut down. This resulted in "massive," but unspecified damage.

The security and industrial control systems (ICS) community has given significant attention to Stuxnet, launched late 2007 or early 2008, and the weapons-grade malware attack that sabotaged centrifuges at an Iranian uranium enrichment facility. Since that attack, discovered in 2010, the security community has predicted that more "destructive" attacks were on the horizon. With the nature of ICS and the management processes typically surrounding them, critical infrastructure (such as power and energy) if similarly attacked, could have a much wider degree of human and societal impact than what resulted at a single steel plant.

[1] "The State of IT Security in Germany 2014," English version available at https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile.

What has been disclosed about the steel mill attack indicates that the attackers came in through the business network via spear-phishing[2] then successfully worked down through the production network to the controllers that operate the plant. Through sending targeted email messages that were cloaked as legitimate correspondences, the attackers were able to inject malware into key systems to gain multiple points of entry and exploration. The attackers were credited with the exploration of a "multitude" of systems including the ICS portion of the network.

The report states, "Failures accumulated in individual control components or entire systems." As a result, the plant was "unable to shut down a blast furnace in a regulated manner," which resulted in "massive damage to the system."

The report also states the attackers appeared to possess advanced knowledge of industrial control systems: "The know-how of the attacker was very pronounced not only in conventional IT security but extended to detailed knowledge of applied industrial controls and production processes."

There is no indication as to how long the attackers were in the systems or if the disablement of the shutdown procedure was intentional or just an accident. The report does, however, give us a stark wakeup call that while expertly crafted weaponized malware like Stuxnet can most certainly cause physical damage to ICS systems, even an inexperienced or tool-driven hacker can do severe damage to an accessible critical infrastructure system.

Risk Assessment and Management Questions and Techniques

The following text is drawn from another EWI work in progress, "Cybersecurity Risks and Rewards," available as an accompaniment of this working paper for this CIRP Breakthrough Group:

The CEO should start by finding out how well his risk management team understands the cybersecurity risk landscape. One way to get there is to ask five key cybersecurity risk questions. These questions are not much different than the questions one might ask about other common business risks, and that is the point. As these questions confirm, managing cybersecurity risk is like managing other risks. It requires a common sense approach and reliance on technical expertise that the CEO may not have.

Experience teaches that most companies are unable to provide convincing answers to questions 3, 4 or 5. The cybersecurity risk landscape is very complex, and new risks arise regularly. Residual risk is thus somewhat open-ended. But known residual risks are identifiable. Similarly, prioritization of investments in cybersecurity is difficult because of the relative immaturity of the field. There is little data to support a quantitative tradeoff between, for example, training employees about malicious attachments versus purchasing a better firewall.

The most important thing to remember is that the answer to question 1, "What are we trying to protect?" defines the answers to all the other questions!

1. What key information and technology assets are we trying to protect?
2. What are the major cybersecurity risks that could affect our business operations and profitability?
3. What techniques are we using to mitigate those risks?
4. What residual risks remain after we have applied those techniques?
5. How did we decide where to prioritize our risk management expenditures and efforts

Discussion Questions

What are the critical success factors for the platform?
Towards what infrastructures should outreach focus first? Toward which countries?
What other organizations should EWI leverage to ensure rapid progress?
How will we know whether the platform is successful?

[2] Spear phishing is an email that appears to be from an individual or business that you know; but, it isn't. The victims are asked to click on a link inside the email that allows the attacker to insert himself inside the enterprise's systems.

Cybersecurity Risks and Rewards
How Much Should CEOs Worry About Cybersecurity?
What Should CEOs Do to Minimize Risk?

A Working Paper of the EastWest Institute Breakthrough Group
Strengthening Critical Infrastructure Resilience and Preparedness

Information and communications technology and connecting to the Internet are indispensable tools for business today. They provide essential economic and operational benefits. But they also create risks that must be managed.

Operating a business means taking risk. Without risk, there is no return to shareholders. Businesses face a variety of risks every day, including natural disasters, unfavorable changes in law or regulation, currency fluctuation, unreliable suppliers, untrustworthy employees and, of course, competition. But taking risks that do not create at least equal benefits—a positive, risk-adjusted return—is just bad business.

Most CEOs understand instinctively, based on experience, how to identify and evaluate most kinds of risks. They know their "risk appetite" and understand that risks may interact with each other. Based on their understanding of the enterprise's risk portfolio, and their sense of the likelihood and impact of any particular risk, CEOs decide what risks to accept, to reduce or transfer to others, and to avoid.

That intuitive understanding may fail, however, when trying to assess a complex technological risk such as cybersecurity risk. For any business today, the likelihood and impact of cyber risks are rapidly increasing. CEOs may well be surprised when a cyber breach occurs, and has a significant impact on the business.

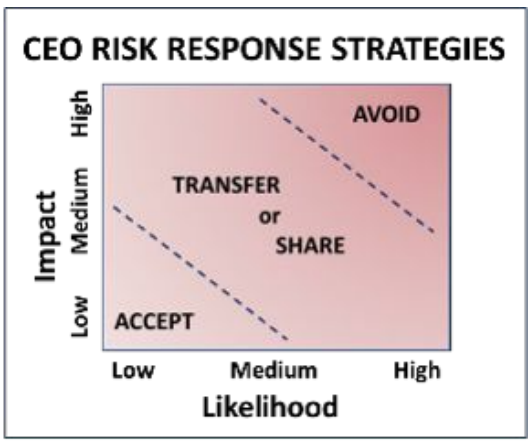
The massive data breach at Target ended the 35-year career of CEO Gregg Steinhafel. His resignation is a stark reminder of the predicament faced by CEOs caught in cybersecurity crises. Cyber attacks are continually becoming more sophisticated, making it difficult for enterprises to stay ahead of the adversary.

Cyber risks can affect business operations by degrading one of the three elements of information or information technology that are critical to the business—confidentiality, integrity and availability.

The ***Cybersecurity C-I-A*** is at the center of cyber risk management.

Damage to the confidentiality, integrity, or availability (the C-I-A) of business information can cause:

- Loss of revenues,
- Reduced profits,
- Damage to reputation,
- Degraded service levels,
- Legal liability.



Different impacts and damage are caused by different attack techniques (see box). Some attackers will use more complex techniques, such as stealing confidential information and threatening to reveal it (extortion).

News reports tend to focus on the more spectacular kinds of attacks—those seeming to come from foreign governments, terrorists or criminals. But most damage comes from competitors, or from service professionals or suppliers who have poor cybersecurity. These trusted business partners can put a company at risk inadvertently.

Types of Attack and Damage	C	I	A
Denial of Service			✓
Theft of Information	✓	✓	✓
Destruction of Information		✓	✓
Modification of Information		✓	
Hijacking of Technology		✓	✓

Inside Threats	Outside Threats
Dishonest or unhappy employees	Competitors
Careless or unaware employees	Service professionals (attorneys, accountants)
Outdated technology	Suppliers, vendors
Weak security implementation	Criminals, terrorists, governments

In addition, many businesses focus primarily on outside threats, when in truth there are as many risks arising from poor practices or malicious individuals inside the company.

Cybersecurity engineers and managers know that it is impossible to avoid all these risks. Defensive technologies and techniques can almost always be defeated by a determined and persistent attacker. Some careless employee will inevitably open an infected file that looks like it came from someone they know. At that point, the enterprise network and the information on it are on the way to compromise.

Step One: The Five Cybersecurity Risk Questions

The CEO should start by finding out how well his risk management team understands the cybersecurity risk landscape. One way to get there is to ask five key cybersecurity risk questions. These questions are not much different than the questions one might ask about other common business risks, and that is the point. As these questions confirm, managing cybersecurity risk is like managing other risks. It requires a common sense approach and reliance on technical expertise that the CEO may not have.

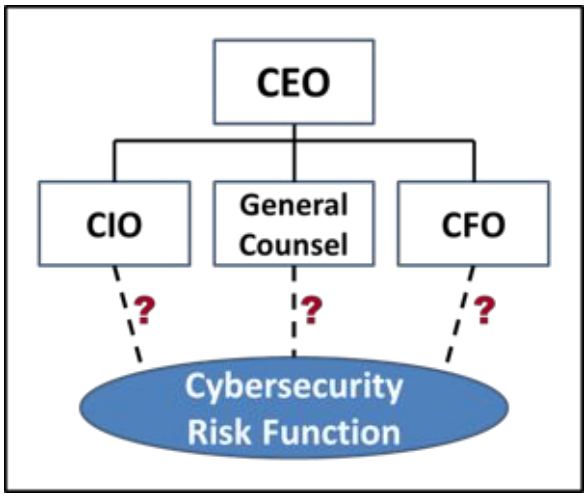
Experience teaches that most companies are unable to provide convincing answers to questions 3, 4, or 5. The cybersecurity risk landscape is very complex, and new risks arise regularly. Residual risk is thus somewhat open-ended. But known residual risks are identifiable. Similarly, prioritization of investments in cybersecurity is difficult because of the relative immaturity of the field. There is little data to support a quantitative tradeoff between, for example, training employees about malicious attachments versus purchasing a better firewall.

The most important thing to remember is that the answer to question 1, “What are we trying to protect?” defines the answers to all the other questions!

1. What key information and technology assets are we trying to protect?
2. What are the major cybersecurity risks that could affect our business operations and profitability?
3. What techniques are we using to mitigate those risks?
4. What residual risks remain after we have applied those techniques?
5. How did we decide where to prioritize our risk management expenditures and efforts?

Step Two: Create the Right Lines of Responsibility

If you asked these five questions to your IT team, you may have run into hesitancy or even resistance in getting definitive answers. For many IT teams, these questions require looking at cybersecurity risk in a new way. You may have discovered one of the most common mistakes companies make: assigning cybersecurity risk management to the Chief Information Officer. This approach can create problems for two reasons.



First, the CIO may not understand the business well enough to evaluate how important it is to safeguard the vulnerable information or technology. Smart firms recognize that the business owner has to get involved because only he or she knows what makes the business operate successfully. The IT team can serve as technical advisors to the business owner, but they cannot usually say what would happen to the business if the key competitive data, such as negotiation strategies or pricing policies, fell into the hands of a competitor. Without that knowledge, the IT team is unlikely to make a correct tradeoff between the costs of security and the costs of just accepting the risk as part of doing business.

Second, the CIO may not be evaluated on his or her security performance. Most CIOs are rewarded for getting technology to the users quickly and cheaply. In this environment, additional security becomes a financial cost that can also cause delays. The CIO's investment in security is likely to be less than what is needed.

As a result, many firms are pulling the cybersecurity function out from under the CIO, and assigning that function to the organization's chief risk management officer—who may also be the General Counsel (who is often responsible for compliance risk) or the Chief Financial Officer (who is often responsible for foreign exchange risk). At a minimum, there needs to be a conversation among senior management about how cybersecurity risk is assigned and the supervisory and reporting lines for that function.

Step Three: Staff for a Comprehensive Approach

Cybersecurity risk is not primarily a technology problem. It requires the involvement of other corporate functions including; human resources—to conduct personnel screening and employee training and awareness; physical security—to prevent theft or compromise by old-fashioned means; a public relations strategy—in case of an incident, legal and compliance expertise; and an understanding of the business value of the information that is being protected.

Best practice suggests forming a cross-disciplinary team to drive the strategy, ensure all aspects are considered and promote buy-in.

Step Four: Ensure Objectivity

Most CEOs do not have the time or expertise to objectively evaluate the performance of their cybersecurity team. Therefore, it is necessary, as with all risk management structures, to ensure that an independent team—that may be internal or external—validates and tests the measures that the cross-disciplinary cybersecurity team has put in place.

Two-Factor Authentication

FIDO 1.0 Final Specifications

FIDO 1.0 Final Specifications Have Arrived

Abstract

The FIDO Alliance has published the final 1.0 specifications. This whitepaper explores the background of FIDO authentication: the needs, benefits, and early deployments.

The Need for a New Authentication Model

During 2014, 783 data breaches occurred and 86 million personal records were stolen; during 2005 through 2014, a total of 4,794 breaches led to a staggering 641 million stolen personal records![3] Clearly, the situation is out of control. Cybercriminals are getting increasingly more sophisticated and are managing to stay ahead of new security technologies, products and services.

There are several fundamental issues with today's authentication infrastructure. Password based authentication relies on centralized stores of user passwords, and a single database breach often results in tens of thousands of stolen credentials. As strong passwords are difficult to remember, most people use weak passwords and/or use the same password at multiple sites - practices that result in security vulnerabilities. In addition, password authentication was developed before mobile devices entered the computing scene, and it is poorly suited for mobile devices, especially from the usability perspective. As a result, many mobile users disable passwords whenever they can, and when forced to use passwords they choose short simple ones (which are also easy to break).

A number of technologies have been implemented to strengthen passwords. Each of them has its own limitations. Hardware tokens provide strong security, and they have been broadly deployed in large enterprises. They have not taken hold with consumers or small businesses, primarily due to high deployment, replacement and support costs of such devices. Another major issue with hardware tokens is that they are very difficult to use with mobile devices. Software tokens are less expensive than hardware tokens but still carry substantial support costs. They are also less secure and have the same usability problem for mobile devices.

One Time Password (OTP) authentication has become popular, especially with the proliferation of mobile devices. A typical use case is to send a one time passcode to a mobile device that the user then enters as a secondary authentication when logging on via a PC. Unfortunately, this technology is ill suited to support authentication from a mobile device as there is typically no additional device where OTB passcodes can be directed.

A common but flawed assumption is that easy-to-use authentication is weak, and strong authentication has to be difficult to use. This model assumes a trade-off curve between usability and security strength (see Figure 1). As a result, strong authentication has been implemented mostly in environments where security is required (or even mandated) such as financials, government, and healthcare. Most other environments are relying on weak password schemes. This situation is leading to a growing number of data breaches and other security disasters. Clearly, something needs to change.

[3] IRTC Data Breach Reports, December 2, 2014

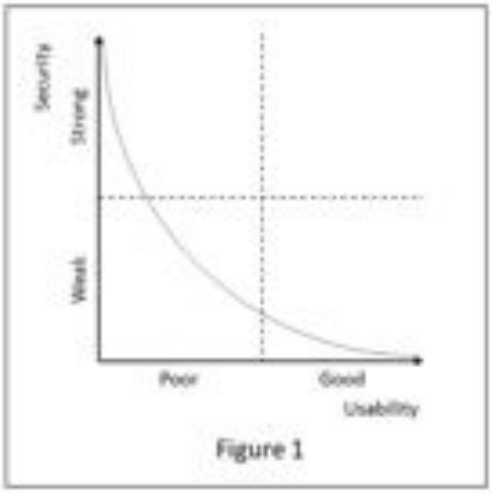


Figure 1

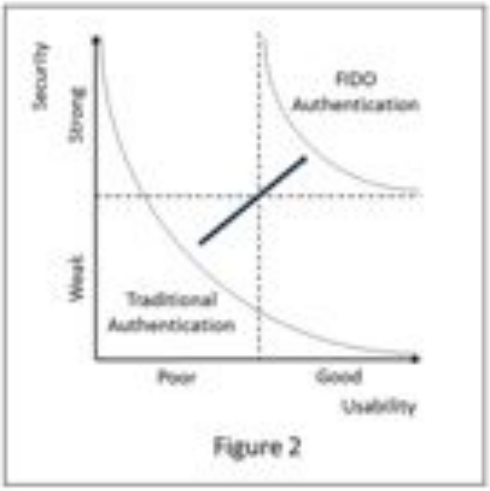


Figure 2

FIDO Authentication Model

The FIDO (Fast IDentity Online) Alliance was formed to create open standards for strong and secure authentication that is also easy to use. It is developing specifications for technologies that will reduce the reliance on passwords, eventually replacing them with other authenticators such as biometrics.

One of FIDO's main design principles is to achieve a satisfactory user experience. In order for authentication to be broadly deployed among consumers and enterprise users, it must be easy to use while providing strong security. This is breaking new ground for authentication, as illustrated in Figure 2.

One of the ways to achieve ease of use in FIDO is to use the same authentication factor (a U2F token or a biometric sensor, for example) seamlessly across multiple services, once initial registration with each service is complete.

Another key design principle is that authentication must protect user privacy. For example, the user's biometric data should never leave the user's device, and any personal data collected during a FIDO operation can only be used for FIDO authentication. Any identification of the user outside of FIDO operations must be prevented. For an in-depth discussion of FIDO privacy principles, please see "The FIDO Alliance: Privacy Principles Whitepaper"[1].

Currently, there are two FIDO protocols – Universal 2nd Factor (U2F) and Universal Authentication Framework (UAF). Both protocols share common FIDO design principles around ease of use and privacy. While U2F and UAF have been developed in parallel and

[1] FIDO Privacy Principles, February 2014

are separate and distinct within the final 1.0 specification, we can expect the two protocols to further develop and harmonize in the future.

Let's take a look at the user experience for U2F and UAF.

U2F strengthens password authentication by adding a physical token. In a typical U2F deployment, a user inserts a U2F token (usually a USB device) into the computer when signing into an online service and taps it when prompted by the browser. The same U2F token may be used to sign in to multiple services (Figure 3).

UAF provides strong authentication without passwords, by using biometrics and other modalities to authenticate users to their local devices, then enabling the devices to authenticate to online services by using cryptography. In a typical UAF deployment, a person simply swipes a finger (or speaks a phrase, or looks at a camera) on a mobile device to login, pay for an item or use another service (Figure 4). Since biometrics and private cryptographic keys are stored on local devices (as a best practice, in hardware tokens or trusted execution environments) and never communicated to the cloud, what's stored on the service provider site is only public cryptographic keys. Even if the service provider site gets hacked, there are no user credentials to be exposed, eliminating the possibility of scalable data breaches.

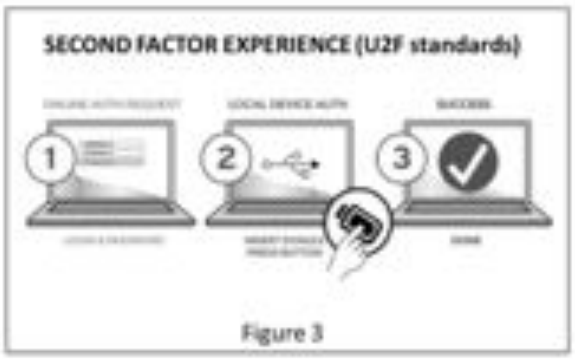


Figure 3

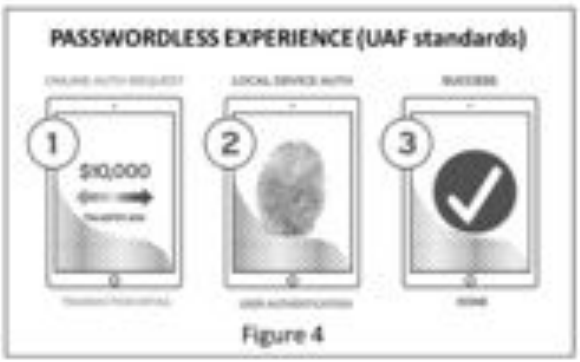


Figure 4

Benefits of FIDO Authentication

FIDO authentication provides a number of powerful benefits to each of its constituencies – consumers, online service providers, and enterprises.

For consumers, FIDO provides strong security with a superior user experience, all while protecting their privacy. It relieves a major pain by eliminating the need to remember many passwords while providing a higher level of security. It has the potential to enable

the use of many mobile applications that are currently hampered by lack of sufficient security.

Consider mobile banking, a use case where a bank acts as an online service provider. According to the Federal Reserve, "concerns about the security of the technology were a common reason for not using mobile banking or mobile payments (69 percent and 63 percent, respectively, of non-users)" [3]. With the FIDO authentication model, authentication from mobile devices is secured with low added cost or complexity.

According to a 2014 study by Axil Partners[4], 60 percent of smartphone or tablet owners who switched primary banks reported mobile banking capabilities as "important" or "extremely important" in their decision to switch, up from 48 percent in a similar survey in the first half of 2013. Clearly, new services such as mobile banking provide one of the largest potentials for differentiation and growth in the banking industry. Yet there are currently no good solutions that can be effectively implemented to enable secure consumer authentication from mobile devices. For banks and others providing high value mobile services, FIDO represents a major opportunity for differentiation and growth. FIDO has the potential to provide similar benefits for service providers in payments, consumer web services, and other industries.

Enterprises also stand to benefit from FIDO protocols. While strong authentication has been deployed by many large enterprises, it is typically implemented via hardware tokens that carry high acquisition costs. According to Gartner[5], average enterprise authentication implementation for a large enterprise in 2014 was priced at $189,000. In addition, a 2014 survey found that companies lose $420 of productivity annually per employee due to struggling with passwords.[6] FIDO can significantly reduce these costs while improving security.

The FIDO Alliance and FIDO Deployments

The growth of internet technologies and mobile devices have made strong online authentication an increasingly important requirement. Yet, as described earlier in this paper, strong authentication solutions have been complex, expensive and difficult to use. The FIDO Alliance was conceived to transform the nature of online authentication by creating a new model of stronger and simpler authentication. Back in 2009, Ramesh Kesanupalli (then CTO of Validity Sensors) had a conversation with Michael Barrett (then CISO of PayPal). Ramesh proposed to "fingerprint enable" PayPal, and while Michael was intrigued with the idea he expressed the need for such solution to be vendor agnostic and

[3] Consumers and Mobile Financial Services 2014, Board of Governors of the Federal Reserve System, March 2014
[4] AlixPartners Mobile Financial Services Tracking Study, March 12, 2014
[5] Gartner Magic Quadrant for User Authentication, 1 December 2014
[6] Survey by Widmeyer sponsored by Centrify Corporation, 2014

standards based. The conversations progressed on from there, more experts got involved, and eventually the FIDO Alliance with six founding members was formed in the summer of 2012 and publicly launched in February 2013.

As the vision of transforming online authentication appealed to many industry players, the Alliance experienced explosive growth, adding around 10 members per month to grow to over 150 members strong. Leading online service providers, financial institutions and technology companies joined the Alliance and contributed to the development of FIDO specifications. In February 2014, the Alliance issued draft specifications for public review, and in December 2014, final 1.0 specifications were made available.

In parallel with the specifications work, several mass-scale FIDO deployments were launched in the market during 2014. At the Mobile World Congress event in February 2014, PayPal and Samsung announced[7] the first FIDO deployment, a collaboration that enables Samsung Galaxy S5 users to login and shop with the swipe of a finger wherever PayPal is accepted. The Samsung Galaxy S5 device is equipped with a fingerprint sensor from Synaptics. PayPal and Samsung selected[8] the Nok Nok Labs S3 Authentication Suite to enable the new payment system. The new service became available in April 2014. In September 2014, Alipay also selected[9] Nok Nok Labs to enable secure online payments via the fingerprint sensor on the Samsung Galaxy S5.

In October 2014, Google launched[10] support for the U2F protocol in its Chrome browser, which set the stage for the world's first deployment of FIDO U2F authentication. With this deployment, Google Chrome became the first browser to implement FIDO standards. In this use case, when signing into a Google Account, the user simply inserts a Security Key into their computer's USB port and taps it when prompted. Users can buy a compatible Security Key from any tested and approved FIDO Ready™ U2F vendor (currently, Yubico and Plug-up).

With the final 1.0 FIDO specifications available and with multiple mass-scale FIDO deployments launched, it is clear that the FIDO Alliance is picking up steam. More important, the new authentication model is changing the world – protecting consumers, reducing the cost of exposure to breaches for online service providers, and lowering infrastructure cost and complexity for enterprises.

---

[7] The FIDO Alliance Announces First FIDO Authentication Deployment, February 24, 2014

[8] Samsung and PayPal select Nok Nok Labs to power the first FIDO Ready Authentication Ecosystem, April 22, 2014

[9] Alipay Selects Nok Nok Labs to Power First FIDO Ready™ Authentication Ecosystem in China, September 17, 2014

[10] Google Launches Security Key, World's First Deployment of Fast Identity Online Universal Second Factor (FIDO U2F) Authentication, October 21, 2014

Increasing the Global Availability and Use of Secure ICT Products and Services

Increasing the Global Availability and Use of Secure Information and Communication Technology (ICT) Products and Services

An EastWest Institute Breakthrough Group

Executive Summary

For more than three decades, the EastWest Institute (EWI) has been an independent and trusted institution, providing thought leadership and mobilizing resources to address some of the most critical security issues facing the world. It brings together key leaders, policy makers, and groundbreaking innovators to develop new solutions to today's daunting challenges.

In 2009, EWI established the Global Cooperation in Cyberspace Initiative to formalize its work on cyberspace issues. As part of that initiative, EWI established seven Breakthrough Groups, each devoted to a specific focus area. This document pertains to the Breakthrough Group (BG) entitled: "Increasing the Global Availability and Use of Secure Information and Communication Technology (ICT) Products and Services."

This BG's objective is to enhance cybersecurity for governments and enterprises globally by enabling the availability and use of more secure ICT products and services. For stakeholders in the ICT supply chain, the BG will promote the use of recognized and proven international standards and best practices that improve product and service integrity. For buyers of ICT, the BG will work to foster the use of procurement practices that are founded on recognized and proven standards and best practices for secure ICT. We will also work to prevent, and where necessary, break down trade barriers so that buyers can identify and utilize trusted providers regardless of their locale.

The purpose of this document is to inform interested parties of this group's efforts, facilitate dialogue and engagement and build momentum towards our objectives. A key indicator of progress will be when guidance or requirements for governments' and critical infrastructure enterprises' procurements integrate recognized standards and practices for integrity and assurance, ultimately helping to enhance the cybersecurity of their systems and operations.

The Challenge

While governments and enterprises around the globe depend on ICT products and services, they are increasingly aware of and concerned about cyber risks. The challenges associated with improving cybersecurity and providing ICT products and services that have sufficient integrity to support these users' critical operations are enormous. One challenge derives from the nature of the ICT marketplace, which thrives in part because technological innovation and development leverages resources—cyber, physical and human—from all over the world.

This global approach provides economies of scale and efficiencies, driving down costs and enabling people and organizations around the world to use and realize the benefits of ICT products and services. However, the sheer number and diversity of individuals, entities, services, and components involved in the technology lifecycle—that includes design, development, deployment, configuration, and operation of ICT—also introduces risks. In the face of more and more serious and dynamic cyber threats, governments and enterprises are increasingly uncertain about whether the global ICT market is driving enough meaningful progress on security and assurance of ICT products and services and their underlying supply chains.

This environment of uncertainty and mistrust has contributed to a growing number of countries proposing or implementing protectionist initiatives as they seek to manage security concerns related to their government and critical

infrastructure operations. Unfortunately, initiatives that focus on promoting local solutions, such as country-specific regulations and bans on foreign products, inevitably raise costs. They are also likely to increase security risks by limiting access to secure ICT and innovations that develop in the global marketplace. Finally, these initiatives may create trade barriers that have problematic economic effects beyond the ICT security market.

Countries should instead foster and maintain an environment that promotes innovation and healthy competition, enabling the development of and access to the most secure technology, now and for years to come. To do so, they should use risk-informed, fact-based procurement practices founded on widely recognized international standards and best practices and objective conformance regimes, which countries can agree to follow and implement transparently. With such a regime in place, ICT providers, component suppliers, integrators, and resellers that adhere to established global standards or certification programs could be recognized as trusted sources—regardless of the country in which they're incorporated or in which they develop, buy, assemble, or operate their products and services. This approach would not only level the playing field for ICT providers globally but also enable more effective cyber risk management and better security.

Buyers of ICT products and services should also be made more aware of and informed about what they should consider consistently asking of, or requiring from, their suppliers. To date, the demand side of the global ICT marketplace has not adequately incentivized ICT providers to integrate increased security. Too often, ICT buyers in both governments and industry do not know what to request or require from providers to improve the security of the products and services that they use. As a result, while some ICT providers are using standards and best practices to improve security and integrity, many do not. Instead, ICT buyers need to consistently demand and incentivize increased security, understanding the risks facing their organizations and defining requirements that are proportionate to the risks that they choose to manage. By asking informed questions and making commercially reasonable demands of ICT providers, buyers can significantly reduce the risk of a range of cyber threats.

The Problem Space & the Stakeholders

Key issues in this problem space include the availability of and access to secure ICT products and services and buyers' ability to procure and use those products and services:

ICT buyers' use of secure ICT products and services:

- Misinformed political and regulatory forces can skew security purchases that would otherwise be risk-informed and market-driven. For instance, restricting ICT purchases based on country of origin inhibits ICT buyers' ability to acquire the most innovative, affordable, and secure products and services.
- Governments have numerous, often conflicting roles as users, protectors, and exploiters of technology, complicating the exchange needed to align market supply and demand.

Availability and access to secure ICT products and services:

- Existing ICT product and services assurance standards and best practices do not scale to accommodate varying levels of risk tolerance and objectives.
- Market demand has not adequately informed and incentivized ICT providers to build security and integrity into their products and services. In addition, inconsistent demands from ICT buyers leave providers facing multiple, disparate, and inadequate signals about which standards might be considered appropriate.

Numerous stakeholders should cooperate to align supply of and demand for secure ICT products and services. A few of the major stakeholders and their potential risks are listed below:

- ICT providers, including original equipment manufacturers (OEMs), hardware and software component suppliers, integrators and resellers.
- ICT buyers, including government, industry and individuals.
- ICT policy influencers, including nonprofits, researchers and standards organizations.

Principles and Approach

This BG is initially taking a two-pronged approach to this problem, focusing on both ICT providers and buyers. Two sets of complementary principles underpin this approach:

1: Supply Side Principles – providers of ICT need:

- An open market that fosters innovation and competition.
- A level playing field for ICT providers, regardless of locale.
- Broader use of a set of scalable and proportionate standards and best practices for security and integrity.
- Buyers of ICT to use procurement processes that utilize fact-driven, risk-informed and transparent requirements.
- Streamlined, agile, and scalable international standards and approaches to conformance.
- A commitment by governments and ICT providers to avoid requirements or behavior that undermines trust in ICT (e.g., by installing back doors).

2: Demand Side Principles – buyers of ICT need:

- Tools and approaches to assess risk.
- A comprehensive understanding of lifecycle costs for ICT to inform decisions not only based on lowest initial costs but also on best overall value.
- Methods to develop and implement consistent procurement requirements appropriate to assessed risks.
- A set of providers recognized as conforming to international standards and best practices for product and service integrity.

Based on these principles, the BG's approach includes providing guidance to:

- ICT providers—regarding how their products, services, and development lifecycles can demonstrate security and integrity by utilizing appropriate and applicable standards, best practices and conformance approaches.
- ICT buyers—regarding what they should be asking for, or requiring from, their providers to align ICT product and service security and integrity to risk tolerance.

Plan

To provide guidance according to the above-described approach, five activities are planned:

1) Collect

From ICT providers, this BG will collect information regarding the standards, best practices, and technologies they use or don't use and their reasoning for doing so. From ICT buyers, this BG will collect input regarding how they assess risks, including ICT supplier risk, and the methods they use (e.g., standards and best practices, contractual requirements and conformance) to manage those risks. Throughout this phase, existing and emerging international standards and best practices for assurance and integrity (e.g., ISO 27036 and 27034, The Open Group's Open Trusted Technology Provider Standards (O-TTPS) also known as ISO DIS20243, Common Criteria and FIDO) will be inventoried, and any supply side gaps will be identified. Likewise, emerging risk management approaches (e.g., NIST Cybersecurity Framework and Huawei's Cybersecurity Perspectives—Top 100 Requirements white paper) will be inventoried, and any demand side gaps will be identified. This phase is planned to be completed by Q3 2015.

2) Aggregate

The BG will aggregate and, whenever feasible, align supply side standards and best practices with risk management approaches collected from the demand side. This list of aggregated standards, best practices, approaches, and mechanisms is intended to help facilitate alignment of ICT providers in developing and ICT buyers in procuring products and services consistent with their levels of risk tolerance. This phase is planned to be completed by Q4 2015.

3) Customize

The BG will customize the aggregated list of standards, practices, and risk management approaches to enable communities of ICT buyers with similar but unique needs to articulate sector-specific implementations. Published as separate and customizable references or guidance documents, the aggregated lists of supply side standards and best practices and demand side approaches and mechanisms will be applicable to the needs of entities that face similar risks, such as the banking and public sectors. This adaptability will ease implementation with the goal of increasing usability. This phase is planned to be initiated by Q1 2016.

4) Formalize

The BG will integrate customized guidance into the methods of evaluation that key ICT buyers use to determine from which providers they will procure secure ICT products and services. In addition, in contracting with providers, ICT buyers may reference this BG's guidance documents, and existing or emerging standards documents may reference this BG's sector-specific guidance.

5) Mobilize

The BG will mobilize support for the guidance documents, utilizing our extensive networks in capitals and corporate headquarters around the world, to seek global utilization of this work.

Upcoming Meetings and Events

The below-described events and meetings are planned to facilitate dialogue around this BG's work and to broaden support for its initiatives:

- Conference calls and meetings with the BG, interested parties and recognized experts
- Interactive webinars
- The Global Cyberspace Cooperation Initiative's annual EWI Summit, at which this BG will report back to the plenary.

Get involved

If you are interested in participating in this BG, would like more information, or would like to be informed of upcoming webinars or other EWI events, please contact Ashley Dennee at adennee@ewi.info.

Preliminary Survey Results: Initial Considerations and Conclusions

A Working Paper of the EastWest Institute Breakthrough Group
Increasing the Global Availability and Use of Secure ICT Products and Services

August 5, 2015

The EastWest Institute (EWI) is leading a Global Cooperation in Cyberspace Initiative to help make cyberspace more secure and predictable. As part of that initiative, EWI has established a Breakthrough Group that is working to enhance cybersecurity for governments and enterprises globally by enabling the availability and use of more secure information and communication technology (ICT) products and services. This group also strives to encourage global recognition of a set of principles that should characterize and help to drive the global ICT marketplace toward more secure products and services and greater transparency.

For providers in the ICT supply chain, the group is promoting the use of recognized and proven international standards and best practices that improve product and service integrity. For buyers of ICT, the group is working to leverage the demand side of the ICT marketplace toward greater security. It is encouraging buyers of ICT to be more informed and organized with like-minded buyers, and more consistent in the inclusion of security requirements. It is also working to foster the use of procurement practices that are founded on recognized and proven standards and best practices for secure ICT.

To this end, EWI requested input on a set of principles and a set of questions for buyers and providers that will provide practical guideposts for evaluating and enhancing the security of ICT products and services, which in turn can be used to seek international support by private organizations and governments for these principles and the transparent use of such standards and best practices.

The survey was launched on July 15, 2015. The preliminary results phase ended on August 5. Sixty-three responses were received. The survey remains open at https://www.surveymonkey.com/s/LLN975D. At EWI's New York Summit on September 9, 2015, an updated version of this report will be presented and discussed. The survey was distributed by EWI and the breakthrough group members to several diverse groups, including: government, research and standards bodies, think tanks, NGO's and private industry.

Survey Demographics

Respondents came primarily from companies or organizations with under one thousand employees.[1] The second largest percentage of respondents came from organizations with five to twenty thousand employees.[2] Similarly, organizations with over sixty thousand employees represented 13% of the respondents.

These numbers were unsurprising given that the largest percentage of respondents (25%) came from government organizations. The top five industries cumulatively make up 53% of respondents and are as follows:

Government—25%
Telecommunications—18%
Education—14%
NGOs—12%
Research and Standards—11%

Those that responded to the survey primarily categorized their organization role as an "expert/specialist" or "head of business unit or department" level.[3] There was an equal distribution among respondents from the "owner/executive/c-level," "CISO/CIO/CTO/CRO" and "manager" levels ranging from 11-14%.

[1] 60% based on survey results.
[2] 15% based on survey results.

The majority of survey respondents consider themselves to be primarily buyers of ICT.[4] An additional 23% consider themselves to be equally a buyer and supplier of ICT. Given that only 26% of respondents consider themselves to be primarily suppliers of ICT, it can be concluded that this survey was of greater initial interest to buyers than suppliers. This may help to explain the responses to how risk is approached and requirements are considered.

Findings for Assessing and Prioritizing Risk in the Supply Chain

1. The approach of assessing and prioritizing risk is primarily developed in house with additional and equal use of NIST 800-30, NIST Cybersecurity Framework and ISO 31000.[5]
2. Organizations take varied and often inconsistent approaches to assessing and prioritizing risk.
3. In some industries, an in-house approach coupled with a "build security in" focus is the primary method of assessing and prioritizing risk.[6]
4. Organizations are evenly split on whether they have or have not considered standards and/or accreditation programs. Following this, those that have considered standards and/or accreditation programs primarily reference ISO 27036 or NIST 800-161.[7]
5. Six percent of respondents could not identify with the question "Identify any of the following standards and/or accreditation programs related to supply chain that you have considered or been asked to consider by suppliers" due to general lack of knowledge or scope.
6. Organizations use multiple and varied resources to develop cybersecurity, software assurance and supply chain requirements. The top five are as follows:
    - ISO 27001- 45%
    - NIST CSF- 33%
    - ISO 27002- 30%
    - NIST 800-53- 21%
    - NIST 800-161- 21%
7. Many organizations indicated their support for other resources listed in the survey or identified additional resources that the breakthrough group had not initially considered for inclusion, which serves to highlight the diversity of resources available to and used by organizations. Additional resources that received support in the survey but did not make it into the top five include: COBIT, Germany's Information Security BSI standard; HIPPA, Huawei's Top 100 Requirements; ISO 27034, ISO 27036, The Open Group (O-TTPS) recently approved as ISO/IEC 20243; and PCII. Other resources that were write-ins by respondents include: COPPA (Children's Online Privacy and Protection Act); FERPA (Family Educational Rights and Privacy Act); OWASP OpenSAMM; SP 800-126 Revision2; NIST SP 800-51 Revision 1; and the ITU-T X. 1500 series.
8. Just under half of organizations feel that their procurement requirements provide an opportunity to drive the security of the market.[8] Equally many feel that their organizations' requirements do not provide an opportunity to drive the security market forward, with the specific limiting factors being their relative size and lack of situational knowledge.

Initial Considerations

1. What can this Breakthrough Group do to assist smaller and newer organizations that are interested in driving the security market forward?
2. What correlations could be made by looking at individual responses? In particular, correlations among specific industry approaches would become clearer.

Cybersecurity Requirement Categories

[3] 40% for expert/specialist and 19% for head of business unit or department based on survey results.
[4] 52% based on survey results.
[5] 47% develop their approach in house. A relatively equal distribution of the other three is quantified by a range of 26-29%.
[6] For question 4, a detailed response from the "other" answer choice provided the background for this analysis.
[7] 52% have not considered a specific standards and roughly 48% have either considered or been asked to consider a standards and /or accreditation program. Given, that the question allows multiple results, an exact percentage would require examining individual questionnaires rather than the grouped data.
[8] 48% based on survey results.

This Breakthrough Group asked respondents to rank the relative importance of 11 cybersecurity requirement categories to their organization. "Verification" was deemed the most important with "Laws and Regulations" following closely behind. The remaining requirements were evenly distributed in importance with a standard deviation of 1.36.

The average rankings are as follows:

1st – Verification
2nd– Laws and Regulations
3rd – Third-Party Supplier Management
4th– Delivering Services Securely
5th– Standards and Processes
6th/7th– Strategy, Governance, and Control
6th/7th– Research and Development
8th– Audit
9th– Issue, Defect, and Vulnerability Resolution
10th– Manufacturing
11th– Human Resources

The relatively equal importance of many of these categories, excluding verification and laws and regulations, was supported in the open response question: "Are there other questions you think should have been asked?" Additional responses asked this Breakthrough Group to consider:

- Public-Private partnerships in development and operations.
- Human Resources: Encouraging the training and preparation of educators as smart and informed consumers.
- Questions related to the choice and deployment of cybersecurity technology.
- Questions related to an organization's understanding of Advanced Persistent Threats, how you keep them out and their overall interplay with supply chain.

Initial Considerations

1. What additional categories of cybersecurity requirements should be considered for inclusion?
2. What does it mean that verification and compliance with laws and regulations are the primary drivers of cybersecurity across organizations?

Findings: Supply Side (i.e., what do suppliers of ICT products and services need to hear from their customers?)

This Breakthrough Group asked participants to evaluate the following supply side principles.

- Supply Side Principles—providers of ICT need:
  - An open market that fosters innovation and competition.
  - A level-playing field for ICT providers, regardless of locale.
  - Broader use of a set of scalable and proportionate standards and best practices for security and integrity.
  - Procurement processes that utilize fact-driven, risk-informed and transparent requirements.
  - Streamlined, agile, and scalable international standards and approaches to conformance.
  - A commitment by governments and ICT providers to avoid requirements or behavior that undermines trust in ICT (e.g., installing back doors).
- While all suppliers agree that these principles should be included, 50% felt that additional principles should be considered by this Breakthrough Group, including:
  - Big companies need to have a plan for securing the supply chain as they increase their outsourcing of tasks and projects.
  - Suppliers need to work in tangent with buyers to increase knowledge, concern, and communication regarding the threat landscape and supply chain vulnerabilities, in order to strengthen the acquisition process.

    - Verification and evaluations should be incorporated into SOPs and exercised in a transparent manner.
- The role of assessing cybersecurity risks and determining risk priorities is often conducted in part at the CISO and Risk Team levels.[9]
- Many supply-side-only organizations (vendors) assess risk at multiple levels.[10]
- The majority of suppliers, 83%, of ICT are concerned to some degree about the potential of incorporating third-party supplier components, which may include vulnerabilities; 50% are extremely concerned about this prospect.
- Among suppliers of ICT, there is greater concern for counterfeit components from third party suppliers than for vulnerable component representing a 2% increase in overall concern for third-party supplier that components could be counterfeit. [11]

Initial Considerations

1. What can be learned about the extent and remit of risk assessment for each level of the organization?
2. What strategies are vendors using to minimize risk from third-party suppliers?

Findings: Demand Side (i.e., what do buyers of ICT products and services need to ask their suppliers?)

This breakthrough group asked participants to evaluate the following demand side principles:

Demand Side Principles—buyers of ICT need:

- Tools and approaches to assess risk.
- A comprehensive understanding of lifecycle costs for ICT to inform decisions not only based on lowest initial costs but also on best overall value.
    - Methods to develop and implement consistent procurement requirements appropriate to assessed risks.
    - A set of providers recognized as conforming to international standards and best practices for product and service integrity.

All buyers agreed that these principles should be included, with some comments indicating that additional focus on education of buyers should be considered by this breakthrough group.

Initial Conclusions

1. The categories and questions posed in the survey (based on the Huawei "Top 100") generally align with the buyer and supplier organizations' security requirements, with some suggested additions or changes in emphasis to give greater recognition to governance and human factors.
2. Considerable ambiguity and lack of direction remains in the communication signals between buyer and seller for security requirements, with a great diversity of standards and ad hoc approaches in use.

A more detailed analysis of the survey results, including changes based on the larger sample size, will be presented and discussed at the New York Summit on September 9, 2015.

[9] 83%, for each, based on survey results
[10] This question allowed for multiple responses. With the exception of "Other" all answer choices were chosen at least 3 times.
[11] 86% based on survey results.

Governing and Managing the Internet

Governing and Managing the Internet

A Working paper of the EastWest Institute Breakthrough Group
Governing and Managing the Internet

By:
John E. Savage, An Wang Professor, Computer Science at Brown University
Bruce McConnell, Senior Vice President, EastWest Institute

August 24, 2015

Abstract

Interest in Internet governance (IG) continues to grow. An energizing factor is the expected transfer of supervision of the DNS root zone from the U.S. Department of Commerce to a multi-stakeholder body.[1]

Supervision of the root zone is but one IG issue. Others include combating cyber crime; protecting intellectual property; privacy; surveillance; freedom of speech; bridging the digital divide; national security and the security of hardware, software and networks; resilience of information and information and communications technology (ICT) in the face of disruptions; protection of critical infrastructures and the possibility of using ICT to inflict damage on an opponent. Each of these is an international issue about which states, companies and citizens are rightly concerned; economies could be damaged, sovereignty infringed or security jeopardized by violations of the kind implied.

Discussion in the Breakthrough Group on Governing and Managing the Internet will address the following four questions:

- What is the best way to govern and manage the Internet?
- What are the strengths and weaknesses of multi-stakeholder governance?
- What are the barriers to participation in Internet governance?
- What are your views on the Internet Assigned Numbers Authority (IANA) Transition process?

Below we provide a brief background on each question and elaborate on the question itself. We expect to use the responses received to revise our paper *Exploring Multi-Stakeholder Governance*.[2]

Questions about Governing and Managing the Internet

1. What is the best way to govern and manage the Internet?

Internet governance (IG) includes a large variety of topics. IG includes cyber crime; protecting intellectual property; privacy; surveillance; freedom of speech; bridging the digital divide; managing the domain name system; national security and the security of hardware, software and networks; resilience of information and communications technology (ICT) in the face of disruptions; protection of critical infrastructures and the possibility of using ICT to inflict damage on an opponent.

[1] **NTIA Announces Intent to Transition Key Internet Domain Name Functions**, retrieved August 23, 2015 from http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions. NTIA is the National Telecommunications and Information Administration of the U.S. Department of Commerce.
[2] **Exploring Multi-Stakeholder Internet Governance**, EastWest Institute, 2015, retrieved August 23, 2015 at http://www.ewi.info/idea/exploring-multi-stakeholder-internet-governance

Which is the better way to address Internet governance issues: by creating special-purpose international bodies that deal exclusively with Internet issues, or by adapting existing international bodies to incorporate Internet issues into their remit? If via existing bodies, how would they need to be changed?

2. What are the strengths and weaknesses of multi-stakeholder governance?

Many, but not all, governments have endorsed multi-stakeholder governance[3] (MSG) as their preferred method to manage Internet governance. MSG is a process designed to give stakeholders opportunities to express their views in an open, transparent and inclusive manner. MSG is viewed as a way to energize concerned parties and to bring needed expertise to solve problems.

MSG processes have been used in many fields to address numerous types of problems. However, they are not a panacea. They do introduce problems such as how to define and select stakeholders and how to decide whether or not to use them to advise on issues or to decide them. If the latter is chosen, should the decisions be made by consensus or a vote.

How should stakeholders be determined? Can individuals declare themselves stakeholders? For what IG topics is MSG best suited to make decisions? For each topic, does it suffice for MSG to play a consultative role or should it be used to make decisions? How should decisions be made? How do these issues change when the number of stakeholders is very large?

3. What are the barriers to participation in Internet governance (IG)?

IG involves domestic and international issues with cultural, social, legal, political, economic and technical dimensions. Some areas of IG require stakeholders to have an expertise that may take years to accumulate.

A striking characteristic of the IG issues is their complexity. Is this a barrier to informed participation in international negotiations? Does it give advantage to those with the most experience with these matters? Also, participation in international meetings is expensive. Does this give an advantage to wealthier governments and business interests? Do these two limitations weaken the argument for full stakeholder participation?

4. What are your views on the IANA Transition process?

The IANA[4] Transition concerns the transfer of the National Telecommunications and Information Administration (NTIA) role in handling the IANA naming, numbering and protocol functions from an ICANN department to a potentially different entity.

NTIA asked ICANN to coordinate the IANA transition, stipulating that the transition meet four conditions:

- Support and enhance the multi-stakeholder model;
- Maintain the security, stability and resiliency of the Internet DNS;
- Meet the needs and expectations of the global customers and partners of the IANA services;
- Maintain the openness of the Internet.

NTIA also stated it "will not accept a proposal that replaces the NTIA role with a government-led or an inter-governmental organization solution."

ICANN created the IANA Stewardship Transition Coordinating Group (ICG) and asked it to prepare a proposal for the IANA transition and another on enhancing ICANN's accountability to its community.[5] The latter was assigned to CCWG-Accountability.

---

[3] Hemmati in her book **Multi-stakeholder Processes for Governance and Sustainability**, Earthscan Publishing, 2002, defines MSG as "*processes which aim to bring together all major stakeholders* in a new form of communication, decision-finding (and possibly decision-making) on a particular issue … based on recognition of the importance of achieving equity and accountability in communications between stakeholders and their views. [The processes] are based on democratic principles of transparency and participation and aim to develop partnerships and strengthened networks among stakeholders."

[4] IANA is an acronym for the Internet Assigned Numbers Authority.

Concerning the IANA transition, ICG solicited proposals from the naming, number and protocol communities. While issues have been raised about the latter two responses, the naming response is the most important. A cross-community working group called CWG-Stewardship handled it.

CWG-Stewardship proposed on June 11, 2015 to:

- Move the IANA functions and personnel from an ICANN department to a separate U.S.-based corporation controlled by ICANN (the Post Transition IANA or PTI);
- Create a multi-stakeholder community (MSC) to review the budget of the new entity;
- Decide if the PTI should be replaced.

The MSC would also have the right to review board decisions, recall board members and approve "fundamental" bylaw changes. CWG-Stewardship deferred to CCWG-Accountability on mechanisms it recommends to implement these powers.

On August 5, 2015, CCWG-Accountability proposed mechanisms to empower the ICANN community (the SOs, ACs and NomCom) to exercise the control that CWG-Stewardship requested. It involves creating the position of Sole Member of ICANN under California law.

The Sole Member would have the exclusive power to reconsider or reject ICANN budgets, strategy, operating plans and bylaws as well as to appoint or remove individual board members and/or the entire board.

The Sole Member would be created by ICANN by changing its bylaws. When created, any SO, AC or NomCom can choose to participate in the Sole Member. Another such entity can participate later on a majority vote of the current participants. The Sole Member construction avoids SOs, ACs or NomCom having to acquire legal status in California.

Sole Member participants act by casting five votes in potentially different ways. A majority of votes cast by all participants is needed for most decisions. Some issues, such as changing "fundamental" bylaws, will require a super-majority vote. The ICANN bylaws as well as the operating procedures of participating bodies would be changed to grant them these powers.

> **Is the proposed structure sufficiently multi-stakeholder? Are the stakeholders appropriately defined? Would the new structure be adequately accountable to the stakeholders? Can it address recent generic top level domain (gTLD) disputes, such as .africa, .sucks and .wine? Do you expect the concerns of domain name holders, end users and governments to be properly addressed?**

[5] ICANN defines its stakeholder community to be its three Supporting Organizations (SOs), its four Advisory Committees (ACs), and its Nominating Committee (NomCom). Others, such as subdomain holders and users, are not considered to be stakeholders.

Managing Objectionable Electronic Content Across National Borders

How to Address the Tension Between a Cross-Border Internet and National Jurisdictions?

The Internet & Jurisdiction Project, launched in 2012, facilitates a global multi-stakeholder dialogue process to address growing jurisdictional tensions on the Internet. This neutral platform engages more than 80 key entities from governments, business, civil society, technical community and international organizations to jointly develop and implement a voluntary policy standard: a transnational due process framework for the submission and handling of cross-border requests for domain seizures, content takedown and user identification.

I - A Common Challenge

The Internet allows billions of people from diverse national jurisdictions to cohabit in shared online spaces. These services produce unique social, political and economic benefits for mankind and transnational interactions become the new norm. As a result, more and more diverse social, cultural, religious and political sensitivities and applicable national norms have to co-exist in cyberspace.

The traditional legal system bases jurisdiction on the physical boundaries of national territories. However, Internet platforms and services represent cross-border "digital territories" where users become subject to the "law" of global Terms of Service. This growing dynamic tension increasingly leads to difficult questions of applicable jurisdiction and legal uncertainty for all. Potential conflicts proliferate regarding privacy, defamation, freedom of expression or consumer protection.

Furthermore, as online interactions increasingly involve Internet platforms, technical operators, servers and users based in different physical locations, determining one single applicable law on the basis of traditional territorial criteria becomes difficult or even impossible.

This is especially evident for user-generated content and in particular speech-related issues, for which national rules greatly vary: what is legal in one country can be illegal in others. Moreover, the Terms of Service of private operators can conflict with national laws. Normative collisions between these often incompatible national laws and rules create increasing conflicts between public authorities, Internet platforms or operators, and users across jurisdictions. Such tensions would further increase with the ultimate global penetration of the Internet.

The cost of inaction

Maintaining transnational spaces requires coordinated efforts. However, traditional Westphalian mechanisms of inter-state cooperation are not sufficient. In particular, Mutual Legal Assistance Treaties (MLATs) only deal with relations between states, do not exist among all countries, are most often limited to criminal issues and do not scale up to the growing number of cases that need to be addressed. Meanwhile, a global harmonization of content-related national laws appears unworkable.

In the absence of appropriate frameworks to manage shared online spaces, governments, cross-border platforms and technical operators adopt uncoordinated and potentially incompatible approaches. This includes efforts to enforce local

legislations online either by requiring re-territorialization of cyberspace or by extraterritorial extensions of national sovereignty.

Should this trend continues, it could have the unintended consequence of a creeping fragmentation of the Internet and a forced realignment along national cyberspaces. Such a jurisdictional arms race might threaten the very nature of the Internet as a global distributed network allowing seamless transnational user interactions and services. Not only would this jeopardize the benefits the Internet has brought to mankind, but it would also hamper innovation and economic growth.

A concern for all stakeholders

The current situation represents a rare issue of common concern for all stakeholders:

- Companies find it hard to develop global Terms of Service respectful of a patchwork of national legislations;
- Governments face difficulties of enforcement and fear the impact of other countries' legislation on their own citizens;
- NGOs worry that universal human rights principles are overlooked in the interaction between business and governments;
- Technical operators fear that the neutrality of the DNS layer will be threatened;
- International organizations trying to establish principles in that domain are afraid of ending up competing against each other.

Given the transnational nature of the Internet's logical and application layers, it is not always possible to determine one single applicable jurisdiction. The Internet thus forces actors to manage commons, rather than trying to separate territories. Since no stakeholder group – let alone individual actors - can solve this conundrum alone, the creation of appropriate and viable frameworks requires a multi-stakeholder approach and new modes of cooperation between actors.

II – Due Process and Transparency

The Internet & Jurisdiction (I&J) Project was launched in 2012 to provide a needed neutral platform for a global multi-stakeholder dialogue to address this issue. It responded to the desire of the various actors to explore the elaboration of common framework(s) to enable interoperability between heterogeneous stakeholders and normative orders.

Shared Principles and Norms

Several initiatives by governments, international organizations, business groupings or civil society coalitions have produced proposals for Internet Principles that exhibit a significant degree of convergence. Further consultations revealed operational objectives that could potentially constitute shared norms acceptable to all stakeholders, including:

- Availability: ensuring the broadest possible accessibility of (legal) content
- Granularity: proportionality in any limitation of availability of content
- Transparency: appropriate visibility, traceability and predictability of restrictive measures
- Due Process: clarity of procedures for both platforms and states

Three areas of cooperation

Transnational cooperation is required to enable Digital Coexistence in cross-border spaces, diffuse tensions and avoid fragmentation. Numerous public and private meetings involving key stakeholders held around the world by the I&J Project identified three issue areas to focus upon:

- Domain Seizures
- Content Takedowns
- Access to User Identification

In the absence of international arrangements, requests by public authorities for domain seizures, content takedowns and access to user data are increasingly sent directly, i.e. transnationally, to Internet platforms or operators in other countries. This solution however currently lacks clear procedures and transparency.

To ensure due process in the management of such transborder requests, agreed "procedural interfaces" and norms are needed between states, platforms and operators, as well as users to simultaneously streamline the treatment of the various requests and enable the coexistence of diverse laws in shared cyberspaces.

III – Towards a Transnational Framework

In 2013, participants in the Internet & Jurisdiction Global Dialogue Process identified six fundamental building blocks for such a transnational due process framework: Authentication, Transmission, Traceability, Determination, Safeguards and Execution. Numerous consultations with stakeholders around the world have since then defined corresponding operational components. As a result of further work conducted during 2014 and early 2015, a draft architecture emerged for the intended framework, based on two pillars respectively related to the two phases of request submission and request handling.

Request submission system

Interoperability between heterogeneous actors (public requesters and private requestees) can be achieved via two components establishing due process and transparency by design:

a) A standardized request submission format would structure requests through a shared set of markup tags specifying, among others:

- Authenticated Points of Contact for requesters and requestees
- Request types and categories
- The national legal basis and the procedure followed
- Request details and justification for necessity and proportionality

b) In addition, mutualized databases would automatically collect relevant elements from each request, in order to allow:

- Production of transparency reports by multiple actors from open data statistics
- Progressive compilation of the relevant national laws and procedures
- Request logging

Request handling procedures

Beyond the mechanisms above, participating stakeholders identified the need to further enhance how requests are processed and potential tensions across jurisdictions are handled:

a) The predictability of the decision-making workflow used by platforms and operators in response to transborder requests could be improved via:

- Common procedural norms and standards
- Shared sets of evaluation criteria
- Neutral advisory panels for situations of uncertainty

b) Transnational dispute management mechanisms could better safeguard users' rights and diffuse tensions, via in particular:

- Procedural appeals
- Pre-established channels to foster dialogue between parties in situations of tension

After three years of intense deliberations, the benefits of such a neutral dialogue space have been demonstrated and work is progressing towards practical pilot implementation.

Solutions to the most pressing issues related to Internet governance can only emerge through close dialogue and cooperation among relevant actors. This pioneering effort pragmatically explores new ways to produce the innovative transnational arrangements required by a revolutionary medium that now underpins almost all human activities.

The ongoing commitment of major actors to the Internet & Jurisdiction Process and their willingness to explore practical avenues for enhanced cooperation is deeply encouraging.

More information is available at: www.internetjurisdiction.net

Contacts:

Bertrand de LA CHAPELLE, Director: bdelachapelle@internetjurisdiction.net
Paul FEHLINGER, Manager: fehlinger@internetjurisdiction.net

Government Access to Plaintext Information

Pakistan Bans BlackBerry Services in Privacy Crackdown

Telecommunication authority orders encrypted messaging and internet services to be stopped 'for security reasons'

The Guardian, July 27, 2015

Pakistan has banned BlackBerry's enterprise server and its internet and messaging services "for security reasons" in a crackdown on privacy.

Mobile phone operators were told by the Pakistan telecommunication authority on Friday that the BlackBerry services must be shut down by the start of December.

BlackBerry uses strong encryption – part of its appeal to businesses and users – which prevents law enforcement and intelligence agencies from intercepting messages and snooping on user activity.

"PTA has issued directions to local mobile phone operators to close BlackBerry Enterprise Services from Nov. 30 on security reasons," said a PTA spokesperson.

BlackBerry operates servers through which all internet traffic destined for its smartphones and tablets flows. The servers handle email, messaging, browsing and other communications services, encrypting the data and ensuring greater privacy.

A recent report by Privacy International claims Pakistan's military intelligence agency, the Inter-Services Intelligence (ISI), is seeking to dramatically expand its ability to intercept communications.

Privacy International said the ISI had few legal checks on its surveillance practices.

"Pakistan's intelligence agencies have abused their communications surveillance powers, including by spying on opposition politicians and supreme court judges. Widespread internet monitoring and censorship has also been used to target journalists, lawyers and activists," the report said.

BlackBerry has faced similar problems in the past in India, the United Arab Emirates (UAE), Saudi Arabia and Indonesia.

In 2010, BlackBerry services were banned within the UAE and Saudi Arabia. Bans were lifted in some states but with tightened restrictions. Prime minister David Cameron also considered banning BlackBerry's messaging services within the UK during the 2011 riots.

BlackBerry said: "BlackBerry provides the world's most secure communications platform to government, military and enterprise customers. Protecting that security is paramount to our mission. While we recognise the need to cooperate with lawful government investigative requests of criminal activity, we have never permitted wholesale access to our BES servers."

The National Academies of
SCIENCES • ENGINEERING • MEDICINE

Law Enforcement and Intelligence Access to Plaintext Information in an Era of Widespread Strong Encryption: Options and Tradeoffs

National Academies of Sciences, Engineering, and Medicine
Division on Engineering and Physical Sciences
Computer Science and Telecommunications Board

Terms of Reference for Study

A National Academies of Sciences, Engineering, and Medicine study will examine the tradeoffs associated with mechanisms to provide authorized government agencies with access to the plaintext version of encrypted information. The study will describe the context in which decisions about such mechanisms would be made and identify and characterize possible mechanisms and alternative means of obtaining information sought by the government for law enforcement or intelligence investigations. It will seek to find ways to measure or otherwise characterize risks so that they could be weighed against the potential law enforcement or intelligence benefits. The study will not seek to answer the question of whether access mechanisms should be required but rather will provide an authoritative analysis of options and tradeoffs.

Background and Context

Since the relaxation of export controls on strong cryptography in the 1990s, strong encryption technology has become widely available worldwide. As the unit cost of computing has declined, adding strong encryption imposes a much less significant performance penalty. IT firms have been deploying encryption technologies in response to perceived customer expectations and in an environment now shaped by recent disclosures about intelligence collection and surveillance activities. Strong disk encryption is a default or optional feature on major personal computer and smart phone platforms, a variety of encrypted messaging services are available today, and major email providers have been exploring ways to make encryption easier to use or automatic, on-by-default. Some providers are now offering information and communication systems in which only the user has access to a decryption key.

Faced in the 1990s with the prospect of widespread use of strong encryption, the United States and other nations promoted key recovery mechanisms that would guarantee government access to the unencrypted information. Fundamentally, key recovery systems involve (1) a mechanism external to the primary means of encryption and decryption that allows a third party to access the encrypted information when authorized and (2) the securing of the secret keys from unauthorized use for an extended period of time (the time scale over which the party that encrypted the information wishes to maintain its confidentiality). They also require access to the encrypted communications or stored information.

Today, as strong encryption is becoming more widely available, law enforcement and national security officials are advocating for the creation of features that enable government exceptional access. Officials point to the risks of "going dark" as communications shift away from systems that have established technical and legal access mechanisms, such as the public telephone network, and because the 1994 Communications Assistance

for Law Enforcement Act exempts carriers from helping with encrypted traffic unless they hold the decryption keys. FBI Director James Comey warned in a November 2014 speech that law enforcement investigations would be hampered as companies encrypt more of their services, a view he echoed in March 2015 congressional testimony. Government officials in other countries, such as the United Kingdom, have expressed similar concerns. In a February 2015 speech, ODNI general counsel Robert Litt highlighted these concerns and expressed optimism that "if our businesses and academics put their mind to it, they will find a solution that does not compromise the integrity of encryption technology but that enables both encryption to protect privacy and decryption under lawful authority to protect national security." In a recent speech, NSA director Michael Rogers suggested that key recovery be safeguarded by splitting the secret keys among several government agencies.

Today, the highly globalized nature of the manufacture and deployment of IT systems and services complicates the landscape in several important ways. If the ability of the United States to offer key-escrow schemes was complex in the 1990s-- an offer that ultimately failed-- such ability is no longer an option. Neither is the ability of any one nation to regulate encryption services in a global economy. Global technology firms can also face demands for access from multiple nations, perhaps with different requirements, and thus could be compelled to enable multiple points of access to satisfy multiple third parties, creating an extra burden for industry.

Mandatory key recovery schemes have, from the beginning, been met with opposition on both technical and policy grounds. From a technical perspective, critics argue that encryption infrastructures that accommodate third-party access inherently introduce risks that unacceptably weaken the security of the system as a whole. An obvious new vulnerability created through any such scheme is that the system used to protect the secret keys could itself be the subject of attack as can the processes and procedures used to manage it.

More generally, any key or plaintext recovery mechanism adds system and perhaps cryptographic complexity. The added code inherently adds more risk of bugs and hence security bugs. Furthermore, the "back door" necessary to provide access is by definition a security weakness, in that some external party should have access. It is not obvious that this access path can be secured adequately, especially if complex policies (such as multinational access mediated by geographic constraints) are employed. This consideration is apart from the additional complexity in multiparty cryptographic protocols.

From a policy perspective, critics argue that the government has access to more information than ever even without mandatory access schemes, that these systems would be costly as well as less secure, and that the marginal benefits are not worth the risks to privacy and system security. Critics also warn that U.S. information technology products and services may become less attractive to consumers outside the United States if they facilitate government surveillance.

In essence, critics of government access advocate for encryption that only the user can decrypt, uncompromised by measures to facilitate government access while government officials proposing access acknowledge the value of using encryption to protect confidential information, but nevertheless want to be able to access information of interest without the user's knowledge or consent when properly authorized.

The difficulty in assessing the basis and strength of either of these positions is the comparative risks and benefits have not been rigorously examined. Nor have the technical and nontechnical arguments been clearly distinguished. The study proposed here would objectively consider risks and benefits, and describe a set of alternatives and tradeoffs to inform the policy debate.

Key questions the study might consider include:

Key recovery systems are the easiest methods for government access to the content of communications. What are the risks and costs associated with key recovery systems? How can these be weighed against the potential benefits of these systems for law enforcement and intelligence work?

The ultimate goal is not access to the keys, but access to content. What alternatives to key recovery are available to law enforcement and intelligence agencies? How expensive are such alternatives? Would the alternatives be available for the full set of cases for which surveillance is used? If not, in what ways do alternative investigative techniques potentially compensate for the loss of content collection?

Proposed Activity

The proposed study will involve approximately 6 meetings over a period of 12 months between the first committee meeting and delivery of a final report. A study committee of approximately 12 individuals will be appointed following customary Academies procedures, drawing on an extensive canvassing of the relevant communities and areas of expertise. An initial committee meeting will be used to discuss the charge to the committee and receive briefings. Early meetings of the committee will focus on gathering of testimony and airing of differing points of view. Later meetings will focus on discussion, deliberations, and development of the committee's report. The committee's report will be prepared and reviewed following customary Academies procedures and will be subject to standard report review procedures prior to release.

The proposed study will be conducted on an entirely unclassified basis. The committee’s report will be published by National Academies Press and made available to the public without restriction. Dissemination of the report will be pursued through publication of the committee's report, briefings to the sponsor and other interested parties, derivative publications, and related activities and events.

About the National Academies of Sciences, Engineering, and Medicine

The Academies provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The institution convenes leaders from academe, industry, government, and other sectors to address critical national issues and provide cogent, unbiased advice through an array of approaches for addressing the variety of problems and policy questions that come before it. The end products take many forms: among them, written reports reflecting the deliberations and conclusions of an expert study committee; symposia and other opportunities for decision-makers to discuss national issues; proceedings from conferences and workshops; and “white papers” on policy issues of special interest. Most projects are conducted or overseen by a committee with a diverse range of expertise covering all aspects of the subject.

Department of Justice

STATEMENT OF

SALLY QUILLIAN YATES
DEPUTY ATTORNEY GENERAL
DEPARTMENT OF JUSTICE

AND

JAMES B. COMEY
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"GOING DARK: ENCRYPTION, TECHNOLOGY, AND THE BALANCE BETWEEN PUBLIC SAFETY AND PRIVACY"

PRESENTED

JULY 8, 2015

Statement of
Sally Quillian Yates
Deputy Attorney General
Department of Justice

and

James B. Comey
Director
Federal Bureau of Investigation

Before the
Committee on the Judiciary
United States Senate

At a Hearing Entitled
"Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy"

Presented
July 8, 2015

Good morning, Chairman Grassley, Ranking Member Leahy, and Members of the Judiciary Committee. Thank you for the opportunity to testify today about the growing challenges to public safety and national security that have eroded our ability to obtain electronic information and evidence pursuant to a court order or warrant. We in law enforcement often refer to this problem as "Going Dark".

We would also like to thank this Committee more generally for its continued support for the mission of the Department of Justice. We know that you, like us, take very seriously the role of the Department in protecting the public in a manner that upholds the Constitution and the rule of law.

Introduction

In recent years, new methods of electronic communication have transformed our society, most visibly by enabling ubiquitous digital communications and facilitating broad e-commerce. As such, it is important for our global economy and our national security to have strong encryption standards. The development and robust adoption of strong encryption is a key tool to

secure commerce and trade, safeguard private information, promote free expression and association, and strengthen cybersecurity. The Department is on the frontlines of the fight against cybercrime and we know first-hand the damage that can be caused by those who exploit vulnerable and insecure systems. We support and encourage the use of secure networks to prevent cyber threats to our critical national infrastructure, our intellectual property, and our data so as to promote our overall safety.

American citizens care deeply about privacy and rightly so. Many companies have been responding to a market demand for products and services that protect the privacy and security of their customers. This has generated positive innovation that has been crucial to the digital economy. We, too, care about these important principles. Indeed, it is our obligation to uphold civil liberties, including the right to privacy.

We have always respected the fundamental right of people to engage in private communications, regardless of the medium or technology. Whether it is instant messages, texts, or old-fashioned letters, citizens have the right to communicate with one another in private without unauthorized government surveillance—not simply because the Constitution demands it, but because the free flow of information is vital to a thriving democracy.

The benefits of our increasingly digital lives, however, have been accompanied by new dangers, and we have been forced to consider how criminals and terrorists might use advances in technology to their advantage. For example, malicious actors can take advantage of the Internet to covertly plot violent robberies, murders, and kidnappings; sex offenders can establish virtual communities to buy, sell, and encourage the creation of new depictions of horrific sexual abuse of children; and individuals, organized criminal networks, and nation-states can exploit weaknesses in our cyber-defenses to steal our sensitive, personal information. Investigating and prosecuting these offenders is a core responsibility and priority of the Department of Justice. As national security and criminal threats continue to evolve, the Department has worked hard to stay ahead of changing threats and changing technology.

We must ensure both the fundamental right of people to engage in private communications as well as the protection of the public. One of the bedrock principles upon which we rely to guide us is the principle of judicial authorization: that if an independent judge finds reason to believe that certain private communications contain evidence of a crime, then the government can conduct a limited search for that evidence. For example, by having a neutral arbiter—the judge—evaluate whether the government's evidence satisfies the appropriate standard, we have been able to protect the public and safeguard citizens' Constitutional rights.

The Department of Justice has been and will always be committed to protecting the liberty and security of those whom we serve. In recent months, however, we have on a new scale seen mainstream products and services designed in a way that gives users sole control over access to their data. As a result, law enforcement is sometimes unable to recover the content of electronic communications from the technology provider even in response to a court order or duly-authorized warrant issued by a Federal judge. For example, many communications services now encrypt certain communications by default, with the key necessary to decrypt the communications solely in the hands of the end user. This applies both when the data is "in motion" over electronic networks, or "at rest" on an electronic device. If the communications provider is served with a warrant seeking those communications, the provider cannot provide the data because it has designed the technology such that it cannot be accessed by any third party.

Threats

The more we as a society rely on electronic devices to communicate and store information, the more likely it is that information that was once found in filing cabinets, letters, and photo albums will now be stored only in electronic form. We have seen case after case – from homicides and kidnappings, to drug trafficking, financial fraud, and child exploitation – where critical evidence came from smart phones, computers, and online communications.

When changes in technology hinder law enforcement's ability to exercise investigative tools and follow critical leads, we may not be able to identify and stop terrorists who are using social media to recruit, plan, and execute an attack in our country. We may not be able to root

out the child predators hiding in the shadows of the Internet, or find and arrest violent criminals who are targeting our neighborhoods. We may not be able to recover critical information from a device that belongs to a victim who cannot provide us with the password, especially when time is of the essence.

These are not just theoretical concerns. We continue to identify individuals who seek to join the ranks of foreign fighters traveling in support of the Islamic State of Iraq and the Levant, commonly known as ISIL, and also homegrown violent extremists who may aspire to attack the United States from within. These threats remain among the highest priorities for the Department of Justice, including the FBI, and the United States government as a whole.

Of course, encryption is not the only technology terrorists and criminals use to further their ends. Terrorist groups, such as ISIL, use the Internet to great effect. With the widespread horizontal distribution of social media, terrorists can spot, assess, recruit, and radicalize vulnerable individuals of all ages in the United States either to travel or to conduct a homeland attack. As a result, foreign terrorist organizations now have direct access into the United States like never before. For example, in recent arrests, a group of individuals was contacted by a known ISIL supporter who had already successfully traveled to Syria and encouraged them to do the same. Some of these conversations occur in publicly accessed social networking sites, but others take place via private messaging platforms. These encrypted direct messaging platforms are tremendously problematic when used by terrorist plotters.

Outside of the terrorism arena we see countless examples of the impact changing technology is having on our ability to affect our court authorized investigative tools. For example, last December a long-haul trucker kidnapped his girlfriend, held her in his truck, drove her from State to State and repeatedly sexually assaulted her. She eventually escaped and pressed charges for sexual assault and kidnapping. The trucker claimed that the woman he had kidnapped engaged in consensual sex. The trucker in this case happened to record his assault on video using a smartphone, and law enforcement was able to access the content stored on that

phone pursuant to a search warrant, retrieving video that revealed that the sex was not consensual. A jury subsequently convicted the trucker.

In a world where users have sole control over access to their devices and communications, and so can easily block all lawfully-authorized access to their data, the jury would not have been able to consider that evidence, unless the truck driver, against his own interest, provided the data. And the theoretical availability of other types of evidence, irrelevant to the case, would have made no difference. In that world, the grim likelihood that he would go free is a cost that we must forthrightly acknowledge and consider.

We are seeing more and more cases where we believe significant evidence resides on a phone, a tablet, or a laptop—evidence that may be the difference between an offender being convicted or acquitted. If we cannot access this evidence, it will have ongoing, significant impacts on our ability to identify, stop, and prosecute these offenders.

Legal Framework

We would like to emphasize that the "Going Dark" problem is, at base, one of technological *choices and capability*. We are not asking to expand the Government's surveillance authority, but rather we are asking to ensure that we can continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe.

The rules for the collection of the content of communications in order to protect public safety have been worked out by Congress and the courts over decades. Our country is justifiably proud of the strong privacy protections established by the Constitution and by Congress, and the Department of Justice fully complies with those protections. The core question is this: once all of the requirements and safeguards of the laws and the Constitution have been met, are we comfortable with technical design decisions that result in barriers to obtaining evidence of a crime?

We would like to describe briefly the law and the extensive checks, balances, and safeguards that it contains. In addition to the Constitution, two statutes are particularly relevant to the Going Dark problem. Generally speaking, in order for the Government to conduct *real-time—i.e.*, data in motion—electronic surveillance of the content of a suspect's communications, it must meet the standards set forth in either the amended versions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (often referred to as "Title III" or the "Wiretap Act") or the Foreign Intelligence Surveillance Act of 1978 (or "FISA"). Title III authorizes the Government to obtain a court order to conduct surveillance of wire, oral, or electronic communications when it is investigating Federal felonies. Generally speaking, FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court (FISC), to approve surveillance directed at foreign intelligence and international terrorism threats. Regardless of which statute governs, however, the standards for the real-time electronic surveillance of United States persons' communications are demanding. For instance, if Federal law enforcement seeks the authority to intercept phone calls in a criminal case using the Wiretap Act, a Federal district court judge must find:

- That there is probable cause to believe the person whose communications are targeted for interception is committing, has committed, or is about to commit, a felony offense;

- That alternative investigative procedures have failed, are unlikely to succeed, or are too dangerous; and

- That there is probable cause to believe that evidence of the felony will be obtained through the surveillance.

The law also requires that before an application is even brought to a court, it must be approved by a high-ranking Department of Justice official. In addition, court orders allowing wiretap authority expire after 30 days; if the Government seeks to extend surveillance beyond this period it must submit another application with a fresh showing of probable cause and

investigative necessity. And the Government is required to minimize to the extent possible its electronic interceptions to exclude non-pertinent and privileged communications. All of these requirements are approved by a Federal court.

The statutory requirements for electronic surveillance of U.S. persons under FISA are also demanding. To approve that surveillance, the FISC, must, among other things, find probable cause to believe:

- That the target of the surveillance is a foreign power or agent of a foreign power; and

- That each of the facilities or places at which the electronic surveillance is directed is being used or is about to be used by a foreign power or an agent of a foreign power.

Similarly, when law enforcement investigators seek access to electronic information *stored—i.e.*, data at rest—on a device, such as a smartphone, they are likewise bound by the mandates of the Fourth Amendment, which typically require them to demonstrate probable cause to a neutral judge, who independently decides whether to issue a search warrant for that data.

Collectively, these statutes reflect a concerted Congressional effort, overseen by an independent judiciary, to validate the principles enshrined in our Constitution and balance several sometimes-competing, yet equally-legitimate social interests: privacy, public safety, national security, and effective justice. The evolution and operation of technology today has led to recent trends that threaten this time-honored approach. In short, the same ingenuity that has improved our lives in so many ways has also resulted in the proliferation of products and services where providers can no longer assist law enforcement in executing warrants.

Provider Assistance

Both Title III and FISA include provisions mandating technical assistance so that the Government will be able to carry out activities authorized by the court. For example, Title III

specifies that a "service provider, landlord…or other person shall furnish [the Government]…forthwith all…technical assistance necessary to accomplish the interception." As the communications environment has grown in volume and complexity, technical assistance has proven to be essential for interception to occur. These provisions alone, however, have not historically been sufficient to enable the Government to conduct electronic surveillance in a timely and effective manner.

In the early 1990s, the telecommunications industry was undergoing a major transformation and the Government faced a similar problem: determining how best to ensure that law enforcement could reliably obtain evidence from emerging telecommunications networks. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA requires "telecommunications carriers" to develop and deploy intercept solutions in their networks to ensure that the Government is able to intercept electronic communications when lawfully authorized, although it does not require a carrier to decrypt communications encrypted by the customer unless the carrier provided the encryption and possesses the information necessary to decrypt. Specifically, it requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as "pen register information" or "dialing and signaling information"). CALEA regulates the capabilities that covered entities must have and does not affect the process or the legal standards that the Government must meet in order to obtain a court order to collect communications or related data.

While CALEA was intended to keep pace with technological changes, its focus was on telecommunications carriers that provided traditional telephony and mobile telephone services, not Internet-based communications services. Over the years, through interpretation of the statute by the Federal Communications Commission, the reach of CALEA has been expanded to include facilities-based broadband Internet access and Voice over Internet Protocol (VoIP) services that

are fully interconnected with the public switched telephone network. Although that expansion of coverage has been extremely helpful, CALEA does not cover popular Internet-based communications services such as email, Internet messaging, social networking sites, or peer-to-peer services.

At the time CALEA was enacted, Internet-based communications were in a fairly early stage of development, and digital telephony represented the greatest challenge to law enforcement. However, due to the revolutionary shift in communications technology in recent years, the Government has lost ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA.

The harms resulting from the inability of companies to comply with court-ordered surveillance warrants are not abstract, and have very real consequences in different types of criminal and national security investigations.

Going Forward

Mr. Chairman, the Department of Justice believes that the challenges posed by the Going Dark problem, are grave, growing, and extremely complex. At the outset, it is important to emphasize that we believe that there is no one-size-fits-all strategy that will ensure progress. We have been asked what we should do going forward. We believe we will need to pursue multiple paths:

All involved must continue to ensure that citizens' legitimate privacy interests can be effectively secured, including through robust technology and legal protections.

We must continue the current public debate about how best to ensure that privacy and security can co-exist and reinforce each other, and continue to consider all of the legitimate concerns at play, including ensuring that law enforcement can keep us safe. The debate so far has been a challenging and highly charged discussion, but one that we believe is essential to have. This includes a productive and meaningful dialogue on how encryption as currently

implemented poses real barriers to law enforcement's ability to seek information in specific cases of possible national security threat.

We also cannot lose sight of the international implications of this issue. It is clear that governments across the world, including those of our closest allies, recognize the serious public safety risks if criminals can plan and undertake illegal acts without fear of detection. It is also true that other countries—particularly those without our commitment to the rule of law—are using this debate as a cynical means to create trade barriers, impose undue burdens on our companies and undermine human rights. We should be clear that any steps that we take here in the United States may impact the decisions that other nations take—both our closest democratic allies and more repressive regimes. In addition, any next steps we identify will be more effective if we are working together with our allies, and made more difficult if we are isolated.

We should also continue to invest in developing tools, techniques, and capabilities designed to mitigate the increasing technical challenges associated with the "Going Dark" problem. In limited circumstances, this investment may help mitigate the risks posed in high priority national security or criminal cases, although it will most likely be unable to provide a timely or scalable solution in terms of addressing the full spectrum of public safety needs.

We don't have any silver bullet, and the discussions within the Executive Branch are still ongoing. While there has not yet been a decision whether to seek legislation, we must work with Congress, industry, academics, privacy groups and others to craft an approach that addresses all of the multiple, competing legitimate concerns that have been the focus of so much debate in recent months. But we can all agree that we will need ongoing honest and informed public debate about how best to protect liberty and security in both our laws and our technology.

Conclusion

Mr. Chairman and Ranking Member Leahy, we would like to thank you and the members of this Committee again for your attention to this subject of national importance. While technology may change, our basic commitment at the Department to upholding the rule of law and our constitutional traditions does not. Our goal at the Department is to work collaboratively

and in good faith with interested stakeholders to explore approaches that protect the integrity of technology and promote strong encryption to protect privacy, while still allowing lawful access to information in order to protect public safety and national security.

We would be happy to answer any questions that you may have.

Why the Fear Over Ubiquitous Data Encryption Is Overblown

By Mike McConnell, Michael Chertoff and William Lynn

The Washington Post, July 28, 2015

More than three years ago, as former national security officials, we penned an op-ed to raise awareness among the public, the business community and Congress of the serious threat to the nation's well-being posed by the massive theft of intellectual property, technology and business information by the Chinese government through cyberexploitation. Today, we write again to raise the level of thinking and debate about ubiquitous encryption to protect information from exploitation.

In the wake of global controversy over government surveillance, a number of U.S. technology companies have developed and are offering their users what we call ubiquitous encryption — that is, end-to-end encryption of data with only the sender and intended recipient possessing decryption keys. With this technology, the plain text of messages is inaccessible to the companies offering the products or services as well as to the government, even with lawfully authorized access for public safety or law enforcement purposes.

The FBI director and the Justice Department have raised serious and legitimate concerns that ubiquitous encryption without a second decryption key in the hands of a third party would allow criminals to keep their communications secret, even when law enforcement officials have court-approved authorization to access those communications. There also are concerns about such encryption providing secure communications to national security intelligence targets such as terrorist organizations and nations operating counter to U.S. national security interests.

Several other nations are pursuing access to encrypted communications. In Britain, Parliament is considering requiring technology companies to build decryption capabilities for authorized government access into products and services offered in that country. The Chinese have proposed similar approaches to ensure that the government can monitor the content and activities of their citizens. Pakistan has recently blocked BlackBerry services, which provide ubiquitous encryption by default.

We recognize the importance our officials attach to being able to decrypt a coded communication under a warrant or similar legal authority. But the issue that has not been addressed is the competing priorities that support the companies' resistance to building in a back door or duplicated key for decryption. We believe that the greater public good is a secure communications infrastructure protected by ubiquitous encryption at the device, server and enterprise level without building in means for government monitoring.

First, such an encryption system would protect individual privacy and business information from exploitation at a much higher level than exists today. As a recent MIT paper explains, requiring duplicate keys introduces vulnerabilities in encryption that raise the risk of compromise and theft by bad actors. If third-party key holders have less than perfect security, they may be hacked and the duplicate key exposed. This is no theoretical possibility, as evidenced by major cyberintrusions into supposedly secure government databases and the successful compromise of security tokens held by a major information security firm. Furthermore, requiring a duplicate key rules out security techniques, such as one-time-only private keys.

Second, a requirement that U.S. technology providers create a duplicate key will not prevent malicious actors from finding other technology providers who will furnish ubiquitous encryption. The smart bad guys will find ways and technologies to avoid access, and we can be sure that the "dark Web" marketplace will offer myriad such capabilities. This could lead to a perverse outcome in which law-abiding organizations and individuals lack protected communications but malicious actors have them.

Finally, and most significantly, if the United States can demand that companies make available a duplicate key, other nations such as China will insist on the same. There will be no principled basis to resist that legal demand. The result will be to expose business, political and personal communications to a wide spectrum of governmental access regimes with varying degrees of due process.

Strategically, the interests of U.S. businesses are essential to protecting U.S. national security interests. After all, political power and military power are derived from economic strength. If the United States is to maintain its global role and influence, protecting business interests from massive economic espionage is essential. And that imperative may outweigh the tactical benefit of making encrypted communications more easily accessible to Western authorities.

History teaches that the fear that ubiquitous encryption will cause our security to go dark is overblown. There was a great debate about encryption in the early ’90s. When the mathematics of “public key” encryption were discovered as a way to provide encryption protection broadly and cheaply to all users, some national security officials were convinced that if the technology were not restricted, law enforcement and intelligence organizations would go dark or deaf.

As a result, the idea of “escrowed key,” known as Clipper Chip, was introduced. The concept was that unbreakable encryption would be provided to individuals and businesses, but the keys could be obtained from escrow by the government under court authorization for legitimate law enforcement or intelligence purposes.

The Clinton administration and Congress rejected the Clipper Chip based on the reaction from business and the public. In addition, restrictions were relaxed on the export of encryption technology. But the sky did not fall, and we did not go dark and deaf. Law enforcement and intelligence officials simply had to face a new future. As witnesses to that new future, we can attest that our security agencies were able to protect national security interests to an even greater extent in the ’90s and into the new century.

Today, with almost everyone carrying a networked device on his or her person, ubiquitous encryption provides essential security. If law enforcement and intelligence organizations face a future without assured access to encrypted communications, they will develop technologies and techniques to meet their legitimate mission goals.

–

Mike McConnell is a former director of the National Security Agency and director of national intelligence. Michael Chertoff is a former homeland security secretary and is executive chairman of the Chertoff Group, a security and risk management advisory firm with clients in the technology sector. William Lynn is a former deputy defense secretary and is chief executive of Finmeccanica North America and DRS Technologies.

Computer Science and Artificial Intelligence Laboratory

Technical Report

MIT-CSAIL-TR-2015-026 July 6, 2015

Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, and Daniel J. Weitzner

Keys Under Doormats:

MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS

Harold Abelson, Ross Anderson, Steven M. Bellovin, Josh Benaloh, Matt Blaze, Whitfield Diffie, John Gilmore, Matthew Green, Susan Landau, Peter G. Neumann, Ronald L. Rivest, Jeffrey I. Schiller, Bruce Schneier, Michael Specter, Daniel J. Weitzner

Abstract

Twenty years ago, law enforcement organizations lobbied to require data and communication services to engineer their products to guarantee law enforcement access to all data. After lengthy debate and vigorous predictions of enforcement channels "going dark," these attempts to regulate the emerging Internet were abandoned. In the intervening years, innovation on the Internet flourished, and law enforcement agencies found new and more effective means of accessing vastly larger quantities of data. Today we are again hearing calls for regulation to mandate the provision of exceptional access mechanisms. In this report, a group of computer scientists and security experts, many of whom participated in a 1997 study of these same topics, has convened to explore the likely effects of imposing extraordinary access mandates.

We have found that the damage that could be caused by law enforcement exceptional access requirements would be even greater today than it would have been 20 years ago. In the wake of the growing economic and social cost of the fundamental insecurity of today's Internet environment, any proposals that alter the security dynamics online should be approached with caution. Exceptional access would force Internet system developers to reverse "forward secrecy" design practices that seek to minimize the impact on user privacy when systems are breached. The complexity of today's Internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.

July 7, 2015

Executive Summary

Political and law enforcement leaders in the United States and the United Kingdom have called for Internet systems to be redesigned to ensure government access to information — even encrypted information. They argue that the growing use of encryption will neutralize their investigative capabilities. They propose that data storage and communications systems must be designed for *exceptional access* by law enforcement agencies. These proposals are unworkable in practice, raise enormous legal and ethical questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.

As computer scientists with extensive security and systems experience, we believe that law enforcement has failed to account for the risks inherent in exceptional access systems. Based on our considerable expertise in real-world applications, we know that such risks lurk in the technical details. In this report we examine whether it is technically and operationally feasible to meet law enforcement's call for exceptional access without causing large-scale security vulnerabilities. We take no issue here with law enforcement's desire to execute lawful surveillance orders when they meet the requirements of human rights and the rule of law. Our strong recommendation is that anyone proposing regulations should first present concrete technical requirements, which industry, academics, and the public can analyze for technical weaknesses and for hidden costs.

Many of us worked together in 1997 in response to a similar but narrower and better-defined proposal called the Clipper Chip [1]. The Clipper proposal sought to have all strong encryption systems retain a copy of keys necessary to decrypt information with a trusted third party who would turn over keys to law enforcement upon proper legal authorization. We found at that time that it was beyond the technical state of the art to build key escrow systems at scale. Governments kept pressing for key escrow, but Internet firms successfully resisted on the grounds of the enormous expense, the governance issues, and the risk. The Clipper Chip was eventually abandoned. A much more narrow set of law enforcement access requirements have been imposed, but only on regulated telecommunications systems. Still, in a small but troubling number of cases, weakness related to these requirements have emerged and been exploited by state actors and others. Those problems would have been worse had key escrow been widely deployed. And if all information applications had had to be designed and certified for exceptional access, it is doubtful that companies like Facebook and Twitter would even exist. Another important lesson from the 1990's is that the decline in surveillance capacity predicted by law enforcement 20 years ago did not happen. Indeed, in 1992, the FBI's Advanced Telephony Unit warned that within three years Title III wiretaps would be useless: no

more than 40% would be intelligible and that in the worst case all might be rendered useless [2]. The world did not "go dark." On the contrary, law enforcement has much better and more effective surveillance capabilities now than it did then.

The goal of this report is to similarly analyze the newly proposed requirement of exceptional access to communications in today's more complex, global information infrastructure. We find that it would pose far more grave security risks, imperil innovation, and raise thorny issues for human rights and international relations.

There are three general problems. First, providing exceptional access to communications would force a U-turn from the best practices now being deployed to make the Internet more secure. These practices include *forward secrecy* — where decryption keys are deleted immediately after use, so that stealing the encryption key used by a communications server would not compromise earlier or later communications. A related technique, *authenticated encryption*, uses the same temporary key to guarantee confidentiality and to verify that the message has not been forged or tampered with.

Second, building in exceptional access would substantially increase system complexity. Security researchers inside and outside government agree that complexity is the enemy of security — every new feature can interact with others to create vulnerabilities. To achieve widespread exceptional access, new technology features would have to be deployed and tested with literally hundreds of thousands of developers all around the world. This is a far more complex environment than the electronic surveillance now deployed in telecommunications and Internet access services, which tend to use similar technologies and are more likely to have the resources to manage vulnerabilities that may arise from new features. Features to permit law enforcement exceptional access across a wide range of Internet and mobile computing applications could be particularly problematic because their typical use would be surreptitious — making security testing difficult and less effective.

Third, exceptional access would create concentrated targets that could attract bad actors. Security credentials that unlock the data would have to be retained by the platform provider, law enforcement agencies, or some other trusted third party. If law enforcement's keys guaranteed access to everything, an attacker who gained access to these keys would enjoy the same privilege. Moreover, law enforcement's stated need for rapid access to data would make it impractical to store keys offline or split keys among multiple keyholders, as security engineers would normally do with extremely high-value credentials. Recent attacks on the United States Government Office of Personnel Management (OPM) show how much harm can arise when many organizations rely on a single institution that itself has security vulnerabilities. In the case of OPM, numerous federal agencies lost sensitive data because OPM had insecure infrastructure. If service providers implement exceptional

access requirements incorrectly, the security of all of their users will be at risk.

Our analysis applies not just to systems providing access to encrypted data but also to systems providing access directly to plaintext. For example, law enforcement has called for social networks to allow automated, rapid access to their data. A law enforcement backdoor into a social network is also a vulnerability open to attack and abuse. Indeed, Google's database of surveillance targets was surveilled by Chinese agents who hacked into its systems, presumably for counterintelligence purposes [3].

The greatest impediment to exceptional access may be jurisdiction. Building in exceptional access would be risky enough even if only one law enforcement agency in the world had it. But this is not only a US issue. The UK government promises legislation this fall to compel communications service providers, including US-based corporations, to grant access to UK law enforcement agencies, and other countries would certainly follow suit. China has already intimated that it may require exceptional access. If a British-based developer deploys a messaging application used by citizens of China, must it provide exceptional access to Chinese law enforcement? Which countries have sufficient respect for the rule of law to participate in an international exceptional access framework? How would such determinations be made? How would timely approvals be given for the millions of new products with communications capabilities? And how would this new surveillance ecosystem be funded and supervised? The US and UK governments have fought long and hard to keep the governance of the Internet open, in the face of demands from authoritarian countries that it be brought under state control. Does not the push for exceptional access represent a breathtaking policy reversal?

The need to grapple with these legal and policy concerns could move the Internet overnight from its current open and entrepreneurial model to becoming a highly regulated industry. Tackling these questions requires more than our technical expertise as computer scientists, but they must be answered before anyone can embark on the technical design of an exceptional access system.

In the body of this report, we seek to set the basis for the needed debate by presenting the historical background to exceptional access, summarizing law enforcement demands as we understand them, and then discussing them in the context of the two most popular and rapidly growing types of platform: a messaging service and a personal electronic device such as a smartphone or tablet. Finally, we set out in detail the questions for which policymakers should require answers if the demand for exceptional access is to be taken seriously. Absent a concrete technical proposal, and without adequate answers to the questions raised in this report, legislators should reject out of hand any proposal to return to the failed cryptography control policy of the 1990s.

Global Cyberspace Cooperation Summit VI

New York 2015

EastWest Institute

Global Cooperation in Cyberspace Initiative

SUPPORTERS

Microsoft
Huawei Technologies
Palo Alto Networks
NXP Semiconductors
Qihoo 360
Unisys
CenturyLink

PARTNERS

IEEE Communications Society
Munich Security Conference
The Open Group
The University of New South Wales

New York

Brussels

Moscow

Washington, D.C.

ewi.info
@EWInstitute
#EWIcyber