The G7 Ise-Shima Leaders’ Declaration

The formal communiqué of the meeting contains an introductory paragraph under the heading of Cyber. It is essentially a declaration of principles and contains the following statement: “We strongly support an accessible, open, interoperable, reliable and secure cyberspace as one essential foundation for economic growth and prosperity.” Like many readers of this journal, I have spent my entire career trying to build accessible, open, interoperable, reliable and secure information systems, so I found this acknowledgment by world leaders to be especially gratifying.

The fact that this issue reached the G7 agenda is recognition that cyberspace is not secure; it is insecure enough that their individual and collective interests are imperiled. To put this in context, the other topics addressed in the communiqué are the world economy, migration and refugees, trade, infrastructure, health, women, anticorruption, climate, and energy. Cyber security, as a global concern, has reached quite a high level indeed.

State Behavior

The expanded section of the communiqué elaborates on the theme and contains the following sentence:

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

I have italicized the phrase in the quote because it is so laden with meaning. It calls for “norms,” which I understand to mean standards. I have previously bemoaned the lack of standards for cyber security, so I found this call to be very heartening. These norms will necessarily be “voluntary” because there is no international body to enforce them. But, much as with other supranational declarations...

Steven J. Ross, CISA, CISSP, MBCP

Is executive principal of Risk Masters International LLC. Ross has been writing one of the Journal’s most popular columns since 1998. He can be reached at stross@riskmastersintl.com.
 Nonetheless, there are a few assertions that could have real impact if the G7 countries adhere to them. Chief among these is the statement that “cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law.” So far, there have been no incidents in which cyberattacks have led to shooting, although it is evident that such attacks have been used as adjuncts to warfare already underway, specifically the war between Russia and Georgia in 2008.\(^\text{12}\) Former US Secretary of Defense Leon Panetta has warned of the possibility of a “cyber Pearl Harbor.”\(^\text{13}\) Acceptance of this concern by the other six nations as a casus belli is, to my mind, a necessary, but rather frightening, step.

The Principles contain a statement so specific that its inclusion among the platitudes comes as a bit of a shock: “We also welcome proactive approaches such as ‘Privacy by Design’ which take privacy and protecting personal data into account throughout the engineering process.” The term “Privacy by Design” was originated in the 1990s by Ann Cavoukian, who had been Ontario’s Information and Privacy Commissioner.\(^\text{14}\) It has since become a widely accepted global privacy standard, which the mention by the G7 certainly affirms.

More open to interpretation is the effect on the nations that were not invited to the meeting. Recent research\(^\text{10}\) indicates that, as recently as 2011, none of the G7 nations, except the United States, has been seen to have perpetrated state-to-state cyberattacks. It is not clear, at least to me, whether the G7 statement is a direct rebuke to the countries that engage in cyberattacks or acceptance that at least one of the G7 nations is already carrying out attacks on other states it considers to be adversaries.

**G7 Principles and Actions on Cyber**

Accompanying the communiqué, and referenced within it, is an annex titled “G7 Principles and Actions on Cyber.”\(^\text{11}\) It is a brief document, barely three bullet-pointed pages, that, for the most part, is a recitation of lofty goals with little or no mention of how they would be achieved. These include:

- Fair and equal access to cyberspace
- Respecting and promoting privacy, data protection and cyber security
- A multistakeholder approach to Internet governance
- Promoting and protecting human rights and principles of rule of law online

Nonetheless, there are a few assertions that could have real impact if the G7 countries adhere to them. Chief among these is the statement that “cyber activities could amount to the use of force or an armed attack within the meaning of the United Nations Charter and customary international law.” So far, there have been no incidents in which cyberattacks have led to shooting, although it is evident that such attacks have been used as adjuncts to warfare already underway, specifically the war between Russia and Georgia in 2008.\(^\text{12}\) Former US Secretary of Defense Leon Panetta has warned of the possibility of a “cyber Pearl Harbor.”\(^\text{13}\) Acceptance of this concern by the other six nations as a casus belli is, to my mind, a necessary, but rather frightening, step.

The Principles contain a statement so specific that its inclusion among the platitudes comes as a bit of a shock: “We also welcome proactive approaches such as ‘Privacy by Design’ which take privacy and protecting personal data into account throughout the engineering process.” The term “Privacy by Design” was originated in the 1990s by Ann Cavoukian, who had been Ontario’s Information and Privacy Commissioner.\(^\text{14}\) It has since become a widely accepted global privacy standard, which the mention by the G7 certainly affirms.

The seven national leaders committed their countries to cooperation among national computer security incident response teams. (Well, actually they did not commit themselves. They promised to “endeavor.”) These teams, better known as national CERTs, such as CERT-FR, US-CERT and CERT-UK, are repositories of information about cyberattacks and providers of assistance to those in their nations who have been attacked. International cooperation on cyber security is not new, but recognition of the need for nations to work together to combat cyberattacks by heads of government is new. Just as no one company alone can solve the problem of cyber security (whatever “solve” means in this context), the G7 is saying that no one country can do it either.

The G7 pronouncements on cyber security have not been widely publicized, perhaps because too many editors’ eyes glazed over. They are not a treaty; they
have no force of law; and too few countries agreed to them. But they are an important assertion that the issue of cyber security has reached a level of concern that presidents and prime ministers must address. We security professionals who are doing the work to build adequate protections against cyberattacks may take some comfort in knowing that our efforts are not going unrecognized by the world’s leaders.

Endnotes

2 Safire, W.; Safire’s Political Dictionary, Oxford University Press, UK, 2008
3 Ibid., p. 423
4 Canada, France, Germany, Italy, Japan, the United States and the United Kingdom
6 Full disclosure: My colleague at Risk Masters International, Allan Cytryn, is also an executive board member of the Boston Global Forum, which contributed to the agenda for the Cyber portion of the Ise-Shima meeting, http://bostonglobalforum.org/2016/05/the-bgf-g7-summit-initiative-ise-shima-norms/.
7 Op cit, G7 2016 Ise-Shima Summit
8 Ibid.