information security matters

The G7 and Cyber Security

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

I first learned the term MEGO in a column by the great conservative pundit, William Safire.[1] In his *Safire's Political Dictionary*,[2] he defines the term as an acronym for "my eyes glaze over" and "something that is undeniably important and paralyzingly dull."[3] There are few topics so MEGO as G7 meetings, the gatherings of the leaders of the world's industrialized democracies. You know they happen; you know they are important. But can you name all seven G7 nations,[4] much less their leaders? Do you have any idea what they talk about or accomplish?

With this stirring introduction, your eyes are probably starting to mist and you have your hand on the corner of the page, about to turn. Please stay awhile for a MEGO you should know about. In May 2016, the G7 leaders met in Ise-Shima, Japan, and produced a document that has real meaning for all of us who care about cyber security.

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.*

The G7 Ise-Shima Leaders' Declaration

The formal communiqué of the meeting[5] 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[6] 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[7] 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.[8]

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,[9] 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

(e.g., European Union directives), it is implicit that such norms should be incorporated into the laws and regulations of the nations that have made this commitment. The reference to "responsible state behavior" implies that countries that engage in state-to-state cyberattacks are acting irresponsibly. The qualifier "during peacetime" leaves unsaid that cyberattacks are legitimate actions in time of war.

The G7 leaders restricted themselves to the actions of states, although "non-state actors, including terrorists" are included as well. It is hard to imagine that ISIS or Al Qaeda are going to be impressed by a statement by the leaders of the world's industrialized nations. Perhaps, rather importantly, including non-state actors is a *de facto* declaration of cyberwar on terrorist groups and individuals. That would be just fine with me, since terrorists have clearly declared cyberwar on the world.

More open to interpretation is the effect on the nations that were not invited to the meeting. Recent research[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."[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.[12] Former US Secretary of Defense Leon Panetta has warned of the possibility of a "cyber Pearl Harbor."[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.[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

Enjoying this article?

- **Learn more about, discuss and collaborate on information security management in the Knowledge Center.** *www.isaca.org/Information-Security-Management*

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

1 Safire, W.; "MEGO," *The New York Times*, 6 September 1973, *www.nytimes.com/1973/09/06/archives/mego-essay.html?_r=0*
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
5 G7 2016 Ise-Shima Summit, "G7 Ise-Shima Leaders' Declaration," 26-27 May 2016, *www.mofa.go.jp/files/000160266.pdf*
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.*
9 Ross, S.; "Frameworkers of the World, Unite, Part 2," *ISACA® Journal*, vol. 3, 2015, *www.isaca.org/Journal/archives/Pages/default.aspx*
10 Valeriano, B.; R. C. Maness; "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001–11," *Journal of Peace Research*, vol. 51, iss. 3, 2014, p. 347-360
11 G7 2016 Ise-Shima Summit, "G7 Principles and Actions on Cyber," 26-27 May 2016
12 Markoff, J.; "Before the Gunfire, Cyberattacks," *The New York Times*, 12 August 2008, *www.nytimes.com/2008/08/13/technology/13cyber.html*
13 Department of Defense, "Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City," USA, 11 October 2012, *http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136*
14 Cavoukian, A.; "Privacy by Design: The 7 Foundational Principles," Information and Privacy Commissioner of Ontario, August 2009 (revised in January 2011), *https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf*