THE BGF-G7 SUMMIT INITIATIVE

A BOSTON GLOBAL FORUM REPORT

5/2017

Cyber Conflict and Fake News

Proposals for Consideration at G-7 Summit, Taormina, Italy, May 26-27, 2017

The Boston Global Forum herein submits policy proposals in two areas—cyber conflict and disinformation (fake news)—for consideration at the 2017 G-7 Summit in Taormina, Italy.[1]

1. Taormina Plan to Prevent Cyber Conflict

At the 2016 G-7 Summit at Ise-Shima, Japan, countries affirmed their commitment to support an open, secure, and reliable cyberspace through the application of international law to state behavior in cyberspace, the acceptance of voluntary norms of responsible state behavior in peacetime, and close cooperation among states against malicious cyber activity. Absent from the formal communiqué were statements on cyber conflict, which is a large and growing threat.

Dozens of countries are building military cyber commands. Given the threat of cyber conflict to civilian populations, it is essential to develop ways to prevent the proliferation of cyber weaponry. Thus far, states have shown remarkable restraint in using overt cyber weapons, the exceptions being Stuxnet, used against Iran's nuclear program; Shamoon, used against Saudi Arabia's energy infrastructure; and the Sony attack against free speech. The international community should build upon this restraint and push toward norms that would make the use of cyber weaponry unacceptable.

Cyber weapons are new, not well understood, and if not properly controlled, likely to lead to escalation, with serious unexpected consequences. Software can be used for espionage or to activate or disable a weapon. If a military cannot assess the intent of foreign malware found in its critical computer systems, it might assume the worst. For example, if such software were found in a nuclear missile facility, a commander, fearing that an enemy wants to disable its launch capability, might decide to "use it or lose it."

Targets for cyber attacks could be a) a nation's military command and control system, including military satellites and logistical systems; b) its economy, including its critical infrastructure such as power, water, banking or telecommunications; or c) its system of governance, including its major agencies and electoral systems.

Because national economies are tightly integrated today, cyber conflict, whether it escalates to kinetic warfare or not, could cause serious economic or political damage to a state and put civilians at risk. An attack against a military system is likely to spread to

[1] Contributors to this document are Nazli Choucri, Anders Corr, Michael Dukakis, Ryan Maness, Tuan Nguyen, Thomas Patterson, Derek S. Reveron, John E. Savage, and David Silbersweig.

civilian systems, thereby violating collateral damage norms. The law of armed conflict does apply in cyberspace, but the boundary between war and peace has blurred.

International cooperation is essential to reduce the risk of cyber war by improving transparency across the major powers and enlisting their cooperation against non-state actors and non-conforming states. Risk reduction should begin with identification of critical assets and the risks to which they are exposed. States should then create a system to reduce risks. This will include cooperation with other states and acquiring the necessary expertise to reduce software vulnerabilities. This effort will take the form of information sharing, bilateral and multilateral agreements, articulation of norms of state behavior, and the creation of risk reduction centers that are equipped with "hot lines" to those of other states. **At some point a formal international treaty could be advisable**.

Implementing norms against unacceptable behaviors fosters collective action and strengthens restraint. There may be a time when the international community establishes an international center to monitor and combat cyber threats, conducts attribution analysis, coordinates actions to protect computer systems, and disrupts non-state actors. In the process, states may have to surrender some of their sovereignty.

Cyber risk reduction begins with adherence to the GGE Norms (UN A/70/174), the G7 Ise-Shima norms, and the G20 Norms. However, it goes beyond these and should include the following measures:

- Sharing of **cybersecurity knowledge in depth, include established guidelines.**
- Public identification of **critical national asset classes.**
- **Banning the implantation of software** in these classes during peacetime.
- Sharing of information designed to improve **attribution**.
- Creation and proper manning of **national risk reduction centers.**
- Establishment of **regular security drills between national centers**

The Boston Global Forum calls upon the G7 countries to lead an effort to create a new international institution, to be called the **Taormina Commission** whose purpose is 1) to collect and share with among nations deep computer system security knowledge[2] to greatly improve the security of cyberspace, 2) identify those categories of critical national assets that should not be targeted in peacetime, 3) promote adoption of a norm banning the implantation of any software by one nation in a publicly identified critical national asset class of another nation, 4) facilitate sharing of effective technical means of attribution in cyberspace, 5) encourage the creation of national risk reduction centers, and 6) facilitate international exercises between national risk reduction centers for the purpose of minimize the risk of cyber conflict.

[2] See the talk given in January 2016 by Rob Joyce, now the White House Cyber Security Coordinator, on methods to prevent nation-state hacking: https://www.youtube.com/watch?v=bDJb8WOJYdA

2. Taormina Plan to Combat Fake News

Disinformation, increasingly in the form of fake news, is a growing problem. Fake news consists of pseudo news stories fabricated to be believable. Producers of fake news are typically driven by one of two motives. One is the profit motive. Some social media sites, for example, are created to look like authoritative news sites but in fact publish false sensational stories designed to attract visitors and generate advertising revenue or click bait. The other motive is influence over public opinion. State and state-sponsored actors, as well as motivated individuals and organizations, are the source of most fake news of this type.

Although fake news is not new, the scale of the problem has increased because of technological change. Cyber capabilities and social media have made it possible to distribute disinformation at speeds and volumes not logistically possible in earlier times. And nearly anyone with access to social media can participate. Political instability and opportunity create incentives to engage in the practice, and technological innovations have made it easier to create a multiplier effect.

That fake news is ubiquitous is not in doubt. A study found, for example, that by the end of the 2016 U.S. presidential election campaign the number of Facebook shares, reactions, and comments in response to fake news stories exceeded the number in response to actual news stories. The study did not distinguish the initial sources of the fake news stories, but evidence indicates that Russia was one such source.

Nor is there any doubt that fake news is a threat to orderly society. It can disrupt elections; contribute to public misinformation; sully reputations—not only of individuals, but also of organizations, institutions, and states; and exacerbate ideological and group conflict. For example, Russia Today (RT) engaged in a highly sophisticated cyber disinformation campaign to inflame tensions in Russian-speaking minority regions of eastern Ukraine.

States should commit themselves to combating fake news. The European Union's Eastern Strategic Communications division was created in 2015 to counter Russian disinformation and believes it has evidence of a widespread campaign targeting the European Union. The United Kingdom's Culture Media and Sport Committee created an inquiry on fake news in early 2017. Other states should make a similar commitment.

Political leaders bear special responsibility. Partisan advantage can accrue to political leaders when opponents are the target of fake news. Research indicates, however, that one of the most effective counters to fake news is unified condemnation of such messages by politicians of opposing parties.

States must cooperate in identifying sources of fake news. Although there are literally thousands of such sources, research indicates that a relatively small number of websites generate most fake news, relying on bots and other tools to spread disinformation. A U.K.-based research team, for example, found that many fake Twitter bots are interconnected—the largest cluster included over 500,000 bot accounts.

Pressure should be exerted on social media platforms to detect, identify, and block such sites. Facebook, Twitter, and other platforms have recently taken an interest in combating fake news. Facebook, for example, has partnered with fact-checking organizations to place warnings on fake news items. Questions remain, however, about the potential for scaling up such warnings and how far platforms are willing to go even if other obstacles to scalability are overcome.

News organizations, too, must be encouraged to combat fake news. In many countries, news organizations are facing financial pressures resulting from audience decline, which has weakened their capacity for fact checking, intervening directly to refute false claims, and conducting the well-sourced reporting that can outperform disinformation on social media. Bolstering reliable news organizations is vital to states' national interest.

Technology must also be mustered in the effort to combat fake news. Technology is a breeder of fake news but can also be employed to mitigate it. There is an urgent need to accelerate the development of software that can assist in the detection and disruption of fake news stories.

The effectiveness of fake news rests to a substantial degree on human tendencies, including our tendency to believe information that aligns with our partisan inclinations. The tendency is strong enough that research has found that efforts to combat fake news with counter messages can sometimes backfire, resulting in reinforcement rather rejection of a false belief or perception. Nevertheless, counter messaging can work if conducted properly. Moreover, people can be instructed in safe practices on the Internet such as not sharing messages from unfamiliar sources. Media literacy should be a staple of a twenty-first century education. The Global Citizenship Education Network at UCLA can be a valuable resource as can be the Ethics Code of Conduct for Cyber Peace and Security (ECCC) of the Boston Global Forum.