A New Era of Accountability

PER CONCORDIAM ILLUSTRATION

International legal reform could make states liable for cyber abuse

Dr. Bret Michael and Prof. Thomas Wingfield

The poor quality of security services offered by providers of information and communication technology, or ICT, complicates, even stymies, domestic and international efforts to discourage and lawfully respond to criminal activity, acts of terrorism and armed aggression in cyberspace. As a result, cyberspace has become a parallel universe in which the criminal, terrorist and unlawful combatant can operate with a high degree of impunity. Adding to the challenge, the privacy services provided in the form of user anonymity and data encryption make it difficult for law enforcement, intelligence organizations and militaries to attribute actions, whether lawful or not, to specific individuals or state actors.

An example is the widely reported Stuxnet worm — an integrated set of malware tools used to target a particular type of industrial control system.[1] Stuxnet takes advantage of gaping holes in the specification, implementation and assurance of security policy. The users of Stuxnet were able to exploit these failings to command and control the malware anonymously and to do their bidding remotely. There are few clues as to who developed or used Stuxnet. There is concern that Stuxnet will be used as a template for developing similar-purposed malware that will take advantage of other still-to-be-exploited weaknesses in current and future ICTs, much like the computer viruses and worms of today are variants of those described in Cohen's dissertation[2] and Morris' worm.[3]

However, the accountability problem is more than just technological. There are gray areas in international law, such as in determining the responsibility of a state when nonstate entities take action under the direction, instigation or control of a state's organs. At present, there are conflicting legal opinions about the immunity of the state in such situations. At one extreme, represented by the ruling in *Nicaragua v. United States of America*,[4] the state is immune from accountability. Another, more balanced interpretation is illustrated in *Prosecutor v. Duško Tadic*.[5] Where does this leave us? Given the legal uncertainty in this area, in addition to the ease of conducting covert and clandestine operations in cyberspace, states are incentivized to employ others to act on their behalf, for example, to incite riots or disrupt critical infrastructures in a target state. This lack of legal clarity has two effects: It provides cover for aggressors wishing to push the law beyond its actual limits, and creates uncertainty for law-abiding defenders who may choose to restrain themselves from activities that would protect themselves from lawlessness.

Because of the current technical structures — or lack thereof — and the current legal frameworks, we expect to see more attacks that are difficult if not impossible to attribute via technical means.

To be an internationally wrongful act, a state's action or omission must be attributable to the state and constitute a breach of an international obligation. Moreover, the state is treated as a single entity, so governmental action at any level implicates the state as a whole. International law extends these criteria to the actions of any group whose actions may result in the creation of a new state.

At the international workshop, "Scientific and Legal Problems: Creation of the International Information Security Systems,"[6] we proposed that the international community consider taking some specific initial steps that would make it more difficult for malefactors operating in cyberspace to leverage the gray areas of international law to their benefit.

AGENCE FRANCE-PRESSE

Gen. Keith Alexander, commander of U.S. Cyber Command and director of the National Security Agency, testifies before a Congressional committee on "U.S. Cyber Command: Organizing for Cyberspace Operations" in September 2010.

Analysts at the U.S. National Cybersecurity and Communications Integration Center in Virginia prepare for a cybersecurity exercise.

AGENCE FRANCE-PRESSE

Step One: Debunking myths

We must debunk these three commonly held myths.

One of the three burdens of proof used in criminal law must be met: beyond a reasonable doubt, clear and compelling, and preponderance of the evidence — These standards of proof do not apply to military and intelligence operations. In addition, decision-makers rarely have the luxury of such certainty of attribution before having to act to thwart or respond to attacks, especially in the case of cyberspace, in which there is a high level of time and space compression: Attacks can unfold in milliseconds, and the physical distance between the source of the attack and the target is, for the most part, immaterial.

There are some nontechnical methods to determine the source of a possible attack — Determining the source of an act within the required time to mount an effective response is often impossible because of such factors as spoofing identities and the lack of bilateral or multilateral agreements for sharing data about the paths that messages take in crossing one or more national borders. Given the way the Internet messaging protocols are designed, this is the norm rather than the exception. However, such factors are not showstoppers in determining culpability. There are many other methodologies that may be used to establish culpability, such as those that take advantage of open source, human and signals intelligence. The impossibility of reliable trace-back does not preclude the use of all other sources and methods to build a clear mosaic of responsibility, possibly after the fact.

It is necessary to attribute an act to a state in order to act internationally — On the contrary, individuals and groups may be investigated and prosecuted under another country's domestic law, if one of five conditions is met, commonly referred to as the principles of international jurisdiction:

- **Territorial:** Action in territory, or "substantial effect" in territory
- **Nationality (Active):** Malefactor is your citizen
- **Nationality (Passive):** Victim is your citizen
- **Protective:** Action poses a national security threat to your country
- **Universal:** Crime is so severe that any nation may take jurisdiction (e.g., piracy, slavery, genocide)

Step Two: Developing a framework

We recommended that a legal framework be developed for assessing the intelligence and military activities conducted in physical or cyberspace to reduce the legal uncertainty associated with such activities. As a starting point for discussion and development of such a framework, we proposed creating a two-dimensional space, which would map an intelligence or military activity to a level of state responsibility based on two factors: (1) the degree of state involvement in the activity and (2) our certainty of involvement of the state measured, for example, by determining whether the state is selecting targets, funding the activity, etc.

Step Three: Providing guidance in applying black-letter law

To advance the discussion and formulation of policy on conducting intelligence and military activities in cyberspace, we recommended that realistic examples of activities in cyberspace be given when formulating drafts of black-letter rules at the International Law Commission.[7] Such examples would be of particular value in developing a common lexicon and understanding of issues and solutions among the legal, policy and technical experts involved in discussions of attribution and accountability. At a recent conference in

Moscow, it was evident that participants' interpretations of even commonly used terms varied from one country to another.

The technical challenge

As international discussions ensue, participants in those discussions need to keep in mind that attribution is asymmetric. Parties to communications can have different goals and requirements for attribution, from perfect attribution to perfect nonattribution. Attribution involves a negotiation among the sender, receiver, and any other parties involved in communications and collaborations. In addition, one must have confidence that attribution is accurate and correct. As described above, this is a matter of degree rather than an absolute.

Moreover, attribution will remain a technically challenging problem — there are no silver bullets or quick fixes. For instance, the Internet was conceived without a requirement for user accountability. Retrofitting the Internet with that requirement has proved elusive. Short of starting over, it will require a major shift in the current Internet structure.

We also are repeating similar mistakes in our cellular communications infrastructures. Many of the current cellular infrastructures, for example Global System for Mobile Communications (GSM), rely on one-way authentication between the service subscriber and the service provider, by which the subscriber authenticates himself to the base station, but not vice versa, leaving GSM-based systems open to abuse by malefactors. At the DEF CON 18 exhibition in August 2010, a prominent conference on hacking, a participant with a laptop and antenna demonstrated his ability to turn off cellular encryption in the room by issuing a simple set of GSM instructions.[8]

Users of ICT have two options: (1) trust the infrastructure to deliver the contents of messages correctly or (2) have the sender and receiver agree in advance on how to judge the integrity of messages without relying on knowledge of the path the message followed from its origin to its destination. For option 1, there is little certainty about the integrity of messages when they arrive at their destination, so attribution is problematic. For option 2, technical issues abound, chief among them specifying and correctly implementing the policy and protocols for creation, maintenance or even prevention of strong bindings between the sender and his or her message, as pointed out by Simmons.[9]

Stakeholders aren't limited to the parties exchanging messages. Others interested in the outcome of discussions on state responsibility may include:

- States and organizations directly associated with the sender or receiver
- States and organizations not associated with the sender or receiver, but ones that are interested in some aspect of the provision, negotiation or enforcement of attribution
- States in whose territory messages originate or transit en route to their destination
- Providers of communication services such as Internet access and network/grid infrastructures

Conclusion

As Thomas Buergenthal and Sean Murphy[10] succinctly put it: "even the strongest states have long-term and short-term political and economic interests in an international order in which conflicts are resolved in accordance with generally accepted rules, in a manner that is reasonably predictable, and that reduces the likelihood of resort to force."

What is needed are solutions that are holistic in the sense that they take into account policy, legal and technical considerations, while at the same time are practical to implement and agreeable to states that are mutually distrustful of one another. As the entire history of international relations has played out with these forces at work, the challenges of integrating cyber law, policy and technology are not insurmountable. □

THE ASSOCIATED PRESS

Professor John McCanny is the principal investigator at the Centre for Secure Information Technologies at Queen's University in Belfast, Northern Ireland, which opened in 2009 to spearhead the fight against cybercrime.

1. See http://en.wikipedia.org/wiki/Stuxnet for details about Stuxnet.
2. F. Cohen, Computer Viruses, Ph.D. dissertation, University of Southern California, 1986.
3. J. Markoff, "Computer Intruder is Put on Probation and Fined $10,000," New York Times, May 5, 1990, p. 9.
4. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. U.S.), 1986 International Court of Justice 14, at 100-1 (June 27).
5. Prosecutor v. Dusko Tadic (Judgment in Sentencing Appeals), IT-94-1-A and IT-94-1-Abis, International Criminal Tribunal for the former Yugoslavia (ICTY), January 26, 2000.
6. The workshop was held at Lomonosov Moscow State University in November 2010 as part of the sixth International Scientific Conference on Security and Counter Terrorism Issues.
7. Draft articles on Responsibility of States for Internationally Wrongful Acts, with commentaries, United Nations, in Yearbook of the International Law Commission, 2001, vol. II, Part Two.
8. See http://www.computerworld.com/s/article/9179959/Hacker_snoops_on_GSM_cell_phones_in_demo
9. G. J. Simmons, Subliminal Channels: Past and Present, IEEE European Transactions on Telecommunication, vol. 5, pp. 459-473, 1994.
10. Thomas Buergenthal and Sean D. Murphy, Public International Law in a Nutshell, St. Paul, Minn.: West Group, 4th edition, 2006.

The views and conclusions in this article are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the U.S. Government.