What challenges to (do?) the legal issues regarding cyber operations pose for cyber intelligence activities?

Cyber operations for cyber intelligence activities is a new arena and the legislation regarding them is still maturing. The ability to collect intelligence from foreign powers from a remote location without agents physically located inside that foreign country is still a recent development. A few lines of the correct computer code can collect more intelligence in a few minutes than a single spy could ever achieve in a lifetime.

How should the act of penetrating a targeted network for intelligence collection be viewed legally? Robert Williams argues that the intrusion into a network should be classified as acovert action((Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action, 2011). He provides a definition of covert action: “an activity or activities of the United States Government to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly” (Williams, 2011, p. 1166).

Since no domestic laws specifically govern the American government’s options to respond to a covert action that has targeted it, we must look to international law (Williams, 2011). The practice of intelligence collection has been accepted as a normal function of a nation (Williams, 2011). International law does prohibit “unauthorized entry and use of territory” (Williams, 2011, p. 1176), but there are no prohibitions regarding the collecting of intelligence in international waters, in space, or in cyberspace. Likewise, covert actions are not expressly prohibited under international law.

There are several parallels between the international cyber intelligence activities and domestic cybercrime. In both, one way to view the actions is to treat them as if they were done via traditional “real world” methods (Finklea & Theohary, 2015). Many crimes, like the theft of money, could carry the same punishments no matter if they were perpetrated through the virtual world or by the theft of cash out of a wallet. The result to the victim is the same. Likewise, the theft of state secrets, either performed through cyberspace or physically by a spy in the targeted country, the results are still the same. Countries should respond to the attacking country, if the attack can even be attributed, the same no matter the methods used.

Attribution is also a shared challenge between international intelligence collection and domestic cybercrime (Finklea & Theohary, 2015). Cybercriminals are motivated to hide their true identities, just as countries seeking to gather intelligence are. Law enforcement must put forth an extra effort to identify criminals in cybercrime when compared to a “real world” criminal action. Even if a “real world” criminal is wearing a disguise, attributes about that person can still be identified. The physical location of the criminal alone can be a key piece of evidence. In the cyber world, law enforcement rarely has that benefit. Criminals can easily lie about their location by using proxy servers and services in their actions. The same applies to international intelligence collection.

It may be the case that we do not need many additional laws to address cyber intelligence activities. The laws that exist for traditional intelligence collection activities may be enough.

-Carl

References

Finklea, K., & Theohary, C. (2015).Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement.Washington, D.C.: Congressional Research Service.

Williams, R. D. (2011). (Spy) Game Change: Cyber Networks, Intelligence Collection, and Covert Action.The George Washington Law Review, 1162-1200.