CRS Insights

Information Warfare: Cyberattacks on Sony
Catherine A. Theohary, Specialist in National Security Policy and Information Operations
(ctheohary@crs.loc.gov, 7-0844)
January 30, 2015 (IN10218)

The Department of Defense defines Information Operations (IO) as the integrated employment, during military operations, of information-related capabilities to influence, disrupt, corrupt, or usurp the decision making of adversaries while protecting our own. Closely related to this is the broader concept of Information Warfare (IW), which can include government as well as the private sector and is conducted not only in crisis, conflict, and warfare but also in peacetime, to serve national security and strategic objectives. These activities are conducted in the overall information environment, and can include cyberattacks as well as activities intended to influence a target through the use of information content. Given this, the recent cyberattacks on Sony Pictures Entertainment could be considered an example of an information warfare campaign.

Background

In the run-up to the scheduled Christmas Day release of *The Interview*, a film depicting the assassination of North Korean leader Kim Jong Un, North Korea's Foreign Ministry called the film "the most blatant act of terrorism and war" and threatened a "merciless countermeasure." On November 24, Sony experienced a cyberattack that disabled its information technology systems, destroyed data, and released internal emails. North Korea denied involvement in the attack, but praised hackers, called the "Guardians of Peace," for having done a "righteous deed." Emails followed, threatening "9/11-style" terrorist attacks on theaters scheduled to show the film, leading some theaters to cancel screenings and for Sony to cancel its widespread release, although U.S. officials claimed to have "no specific, credible intelligence of such a plot."

The Federal Bureau of Investigation and the Director of National Intelligence (DNI) attributed the cyberattacks to the North Korean government. During a December 19, 2014, press conference, President Obama pledged to "respond proportionally" to North Korea's alleged cyber assault, "in a place, time and manner of our choosing." President Obama referred to the incident as an act of "cyber-vandalism." On December 20, cyber analysts and news media reported that the North Korean network providing access to the Internet went offline for approximately 10 hours. Many cyber analysts said the disruption pointed to a network attack, although they could not rule out either an overload or a preventive shutdown by North Korea. U.S. officials would not comment on whether this constituted the "proportional response," saying only that some elements of the response would be seen while others would not.

Attribution and Categorization

Although elements of the U.S. intelligence community claimed to have compelling proof of North Korean involvement in the attacks on Sony, many information security experts questioned whether North Korea had the capability to conduct destructive attacks and whether the malware involved contained markers that would definitively indicate North Korean origin. Questions of how to categorize the attacks were also raised, particularly with respect to the actors involved and their motivations as well as issues of sovereignty regarding where the actors were physically located. With the globalized nature of the Internet, perpetrators can launch cyberattacks from anywhere in the world and route the attacks through servers of third-party countries. Was the cyberattack on Sony, a private corporation with headquarters in Japan, an attack on the United States? Further, could it be considered an act of terrorism, a use of force, or cybercrime? Cyberterrorism can be considered "the premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives." Cyberwarfare is typically conceptualized as state-on-state

action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic use of force. Cybercrime includes unauthorized network breaches and theft of intellectual property and other data; it can be financially motivated, and is typically the jurisdiction of law enforcement agencies. In categorizing the attacks on Sony as an act of "cyber vandalism," which typically includes defacing websites and is usually the realm of politically motivated actors known as "hacktivists," President Obama raised questions of what type of response could be considered "proportional," and against whom.

Cognitive Element

Regardless of the level of confidence in attributing the cyberattacks on Sony to North Korea, and independent of the level of damage that Sony suffered, one could argue that the incident represents a successful use of IW to achieve political ends. Some questioned whether North Korea had developed a sophisticated cyberattack force, using these attacks to demonstrate its increasing ability to pursue political goals and thereby raise its profile on the international stage. Others pointed to the common use of proxies or mercenary hackers to conduct relatively simple cyber operations as a form of political protest or "cyber riot." Whether or not the North Korean government conducted the attacks or outsourced to a proxy organization, the cyberattacks in concert with threats of physical destruction affected the decision-making process of a private company, exploited the human element of fear in a civilian population, imposed extra-territorial censorship, and triggered the United States government to respond.

Although the United States did not claim responsibility for the North Korean outage, the lack of denial could suggest the use of strategic ambiguity as a counter-maneuver. One public response to the attacks, referred to by leadership as a "first step," was an executive order imposing new economic sanctions on North Korean entities for "destructive, coercive cyber-related actions during November and December," and a "continuing threat to the national security, foreign policy and economy of the United States." Other officials issued strongly worded declarations: the DNI called these attacks "the most serious yet on U.S. interests," while the leader of U.S. Cyber Command and the National Security Agency (NSA) said that the government should respond more forcefully to fight the perception that there is "little price to pay" for international actors who engage in such activity. Reports surfaced that the NSA had secretly planted malware in North Korean systems in order to track hackers. This leak could also be an IW ploy, designed to create uncertainty in the minds of North Korean leadership regarding their network security.