Congressional Research Service

The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability

Paul K. Kerr
Analyst in Nonproliferation

John Rollins
Specialist in Terrorism and National Security

Catherine A. Theohary
Analyst in National Security Policy and Information Operations

December 9, 2010

Congressional Research Service
7-5700
www.crs.gov
R41524

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

In September 2010, media reports emerged about a new form of cyber attack that appeared to target Iran, although the actual target, if any, is unknown. Through the use of thumb drives in computers that were not connected to the Internet, a malicious software program known as Stuxnet infected computer systems that were used to control the functioning of a nuclear power plant. Once inside the system, Stuxnet had the ability to degrade or destroy the software on which it operated. Although early reports focused on the impact on facilities in Iran, researchers discovered that the program had spread throughout multiple countries worldwide.

From the perspective of many national security and technology observers, the emergence of the Stuxnet worm is the type of risk that threatens to cause harm to many activities deemed critical to the basic functioning of modern society. The Stuxnet worm covertly attempts to identify and exploit equipment that controls a nation's critical infrastructure. A successful attack by a software application such as the Stuxnet worm could result in manipulation of control system code to the point of inoperability or long-term damage. Should such an incident occur, recovery from the damage to the computer systems programmed to monitor and manage a facility and the physical equipment producing goods or services could be significantly delayed. Depending on the severity of the attack, the interconnected nature of the affected critical infrastructure facilities, and government preparation and response plans, entities and individuals relying on these facilities could be without life sustaining or comforting services for a long period of time. The resulting damage to the nation's critical infrastructure could threaten many aspects of life, including the government's ability to safeguard national security interests.

Iranian officials have claimed that Stuxnet caused only minor damage to its nuclear program, yet the potential impact of this type of malicious software could be far-reaching. The discovery of the Stuxnet worm has raised several issues for Congress, including the effect on national security, what the government's response should be, whether an international treaty to curb the use of malicious software is necessary, and how such a treaty could be implemented. Congress may also consider the government's role in protecting critical infrastructure and whether new authorities may be required for oversight.

This report will be updated as events warrant.

Contents

Appendixes

Contacts

Introduction: The Stuxnet Computer Worm[1]

Since the invention of the first computer-assisted industrial control system (ICS) device over 40 years ago,[2] both the technical and national security communities have voiced concerns about software and hardware vulnerabilities and potential security risks associated with these devices. Such concerns have generally involved the infiltration of a computer system for purposes of degrading its capabilities, manipulating data, or using the device to launch cyber attacks on other systems. The Stuxnet worm,[3] which was first reported in June 2010 by a security firm in Belarus, appears to be the first malicious software (malware) designed specifically to attack a particular type of ICS: one that controls nuclear plants, whether for power or uranium enrichment. The malware attacks and disrupts a Microsoft Windows-based application that is employed by a particular ICS produced by the German company Siemens.[4] The worm can be spread through an air-gapped network by a removable device, such as a thumb drive, and possibly through computers connected to the Internet, and it is often capable of remaining hidden from detection. It is difficult to determine the geographic origin of the malware, as cyber attackers often employ sophisticated methods such as peer-to-peer networking or spoofing IP addresses to obviate attribution. Likewise, malware placed on a removable device may contain no signatures that would identify its author. Some security analysts speculate that Stuxnet could have been developed by a Siemens insider who had direct access and knowledge of the system; others contend that the code's sophistication suggests that a nation state was behind the worm's development, either through proxy computer specialists or a government's own internal government and military capabilities.[5]

To date, numerous countries are known to have been affected by the Stuxnet worm to varying degrees of disruption in their technology systems. These include Iran, Indonesia, India, Pakistan, Germany, China, and the United States. A lack of publicly available information on the damage caused by Stuxnet in these countries makes it difficult to determine the malware's potency.

[1] Information contained in this report is derived from unclassified open source material and discussions with senior government officials and industry technology and security experts.

[2] Industrial control systems (ICS) assist in the management of equipment found in critical infrastructure facilities. ICSs include supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and Programmable Logic Controllers (PLC). For additional information on ICS see Guide to Industrial Control Systems, National Institute of Standards and Technology, September 2008, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf.

[3] A computer worm differs from a virus in that the latter requires user action to set in motion of set of potential harmful activities whereas a worm is self-executable and will burrow its way through an operating system until it reaches its intended target.

[4] See ESET Technical Report: Stuxnet Under the Microscope, accessed at http://www.eset.com/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.

[5] For more information on the technical details of Stuxnet, including its discovery, possible origin, level of sophistication, and breadth, see Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Version 1.1, Symantec, accessed at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

The Stuxnet Worm: Possible Developers and Future Users

In attempting to assess the Stuxnet worm's potential targets and ascertain how best to identify and slow progress of its spread to other ICSs, numerous researchers have speculated as to the identity of the software code's developer. To date, no country or group has claimed responsibility for developing what has been termed by some as "the world's first precision guided cybermunition."[6] Given the Stuxnet worm's reported technical sophistication, numerous researchers and media outlets have speculated that a government most likely produced it. According to these accounts, the developer had to be financially well-resourced, employ a variety of skill sets (including expertise in multiple technology areas), have an existing foreign intelligence capability in order to gain access and knowledge of a foreign system, and be able to discretely test the worm in a laboratory setting. Moreover, states appear to possess a motive to develop Stuxnet because, unlike other forms of malware, the worm is not designed to steal information, but rather to target and disrupt control systems and disable operations.[7] Countries thought to have the expertise and motivation of developing the Stuxnet worm include the United States, Israel, United Kingdom, Russia, China, and France.[8]

In addition to speculating on the developer's identity, observers have formulated theories about the worm's intended purpose. For example, some argue that Stuxnet's developer may not have intended the worm to spread beyond its desired target, thus bringing unwarranted attention to this emerging cyber capability.[9] Furthermore, it is likely the developer did not consider the unintended consequence of the worm becoming widely available and subject to manipulation to make it less identifiable and more potent.

A terrorist organization intent on carrying out attacks on a nation's critical infrastructure may also be interested in targeting a type of ICS known as supervisory control and data acquisition (SCADA) systems. It is widely believed that terrorist organizations do not currently posses the capability or have made the necessary arrangements with technically savvy organizations to develop a Stuxnet-type worm. However, the level of attention the Stuxnet worm has received creates a possible proliferation problem and what some have termed a "cyber arms race."[10] The Stuxnet code itself is now freely available on the Internet, as are the particular vulnerabilities it exploits, as well as the web addresses of unsecured SCADA systems.[11] As software developers

[6] Hunting an Industrial-Strength Computer Virus Around the Globe, *PBS Newshour*, October 1, 2010, http://www.pbs.org/newshour/bb/science/july-dec10/computervirus_10-01.html.

[7] Nicolas Falliere, Liam O Murchu, and Eric Chien, W32.Stuxnet Dossier, Version 1.1, Symantec, accessed at http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[8] Theories Mount That Stuxnet Worm Sabotaged Iranian Nuke Facilities, Forbes online, September 22, 2010, http://blogs.forbes.com/andygreenberg/2010/09/22/theories-mount-that-stuxnet-worm-sabotaged-iranian-nuke-facilities/.

[9] Each of the Nations mentioned as a possible developer of the Stuxnet worm have, to varying degrees, had industrial control systems in their country affected.

[10] Warwick Ashford, "Stuxnet worm is prototype for cyber-weapon, say security experts," *Computer Weekly*, September 24, 2010.

[11] SCADA systems can be located via public search engine, says the Industrial Control Systems Cyber Emergency Response Team, InfoSecurity.com, November 3, 2010, http://www.infosecurity-magazine.com/view/13690/scada-systems-can-be-located-via-public-search-engine-says-cert/.

often revise and reformulate existing code, Stuxnet's design revelations may make it easier for terrorist organizations to develop such capabilities in the future. Melissa Hathaway, former Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils, was recently quoted as saying, "Proliferation [of cyber weapons] is a real problem, and no country is prepared to deal with it. All of these [computer security] guys are scared to death. We have about 90 days to fix this [new vulnerability] before some hacker begins using it."[12]

It is also worth noting that, in the future, a non-state actor may not necessarily need to possess the Stuxnet code in order to use the worm. Cybercrime organizations have been said to "rent" networks of infected computers, known as "botnets," for use in politically motivated cyber attacks on government websites and computer networks. It may become possible for organizations to develop and either rent or sell malware such as Stuxnet or access to infected computers for malicious use against government or civilian infrastructure. In addressing concerns about threats emanating from cyberspace from a variety of potential actors, Deputy Defense Secretary William J. Lynn III noted, "Once the province of nations, the ability to destroy via cyber means now also rests in the hands of small groups and individuals: from terrorist groups to organized crime, hackers to industrial spies to foreign intelligence services."[13]

Early reports indicated that the intended target of Stuxnet may have been SCADA-controlled nuclear facilities in Iran that used the Siemens product.[14] If a country developed Stuxnet and the target was a single country's infrastructure, the worm's spread to multiple countries has implications for the lack of precision targeting of cyber weapons, their unknown secondary and tertiary effects, and for the rules of engagement for responding to a cyber attack.

Iran: The Intended Target?

Iran has apparently suffered the most attacks by the Stuxnet worm and, as noted, may well have been its main target. A September 2010 study by Symantec argued that the "concentration of infections in Iran likely indicates that this was the initial target for infections and was where infections were initially seeded."[15] As of September 25, 2010, Iran had identified "the IP addresses of 30,000 industrial computer systems" that had been infected by Stuxnet, according to Mahmoud Liaii, director of the Information Technology Council of Iran's Industries and Mines Ministry, who argued that the virus "is designed to transfer data about production lines from our industrial plants" to locations outside of Iran.[16]

Iranian officials have indicated that the worm infected computers associated with the country's nuclear power plant under construction near Bushehr. Dr. Mohammad Ahmadian, an Iranian Atomic Energy Organization official, stated in October that the worm may have been transferred

[12] John Markoff, "A Silent Attack, but Not a Subtle One," *The New York Times*, September 26, 2010.

[13] Cybersecurity Poses Unprecedented Challenge to National Security, Lynn Says, U.S. Department of Defense, American Forces Press Service, June 15, 2009, http://www.defense.gov/news/newsarticle.aspx?id=54787.

[14] Gregg Keizer, "Iran confirms massive Stuxnet infection of industrial systems," *Computerworld*, September 25, 2010.

[15] Nicolas Falliere, Liam O Murchu, and Eric Chien, *W32.Stuxnet Dossier*, Symantec Security Response, September 2010, p. 7.

[16] "Iran Confirms Cyber Attack, Says Engineers 'Rooting Out' Problem," *Mehr News Agency*, September 25, 2010. Ali Akbar Salehi, the head of Iran's Atomic Energy Organization, stated in an interview published October 8 that the organization "became aware" of the worm as early as July.

to computers at the reactor site via "CDs and Flash memory sticks," adding that the affected computers have since been "inspected and cleaned up."[17] Some of those responsible for transferring the worm were "foreign experts who had been frequenting industrial centres," Iran's minister of communication Reza Taqipur stated in October.[18] Iranian officials have indicated that the reactor, which is not yet operational, has not been affected by Stuxnet.[19] Olga Tsyleva, press-secretary of the Atomstroyeksport, the Russian contractor for the Bushehr project, confirmed October 5, 2010, that the worm had spread to the Bushehr facility's computers but had not caused any damage.[20]

In addition to Liaii's description of Stuxnet's purpose, reports of the Stuxnet infections in Iran have, as noted, fueled speculation that the virus was part of an effort by some countries, including the United States and Israel, to sabotage Tehran's nuclear programs. In addition to the Bushehr reactor, Iran has constructed both a pilot and a commercial gas centrifuge-based uranium enrichment facility near Natanz. [21] Tehran continues enrichment operations at the Natanz facilities, according to a November 23, 2010, report by International Atomic Energy Agency Director-General Yukiya Amano.[22] Uranium enrichment can produce fuel for nuclear reactors, but can also produce fissile material for use in nuclear weapons.

Iran's uranium enrichment facilities seem to be a more likely target for a cyber attack than does the Bushehr reactor. Mark Fitzpatrick, former acting Deputy Assistant Secretary of State for Non-proliferation, argued in September that such an attack would not make sense because the reactor is not a prime proliferation concern, the *Financial Times* reported.[23] Iranian officials have themselves indicated that the Bushehr reactor may not have been the worm's only target. For example, an October 5 statement from Iran's Foreign Ministry spokesman Ramin Mehmanparast appeared to reference Iran's uranium enrichment program.[24] Moreover, Ali Akbar Salehi, the head of Iran's Atomic Energy Organization, suggested September 29 that "enemies" had attempted to infect nuclear facilities other than Bushehr.[25] More recently, some experts have argued that, because Stuxnet was designed to manipulate equipment used in centrifuge facilities, the worm may have been developed to sabotage Iran's enrichment plant.[26] Whether the Natanz facility contains Siemens components that would be affected by the virus is unclear. The presence of such

[17] "Iran's Bushehr Nuclear Plant to Come on Stream in Mid April 2011," *Islamic Republic News Agency*, October 16, 2010.

[18] "Stuxnet Virus Spread Individuals Said Identified by Iran Official," *Islamic Republic of Iran Broadcasting*, October 20, 2010.

[19] Islamic Republic News Agency, October 16, 2010; "Bushehr Reactor to Get Main Fuel in Second Week of October," *Islamic Republic News Agency*, October 5, 2010.

[20] "Fuel Lading at Iran's Bushehr Pant Panned for October - Russian source," *RIA Novosti*, October 5, 2010.

[21] See CRS Report RL34544, *Iran's Nuclear Program: Status*, by Paul K. Kerr. Russia, rather than Iran, is to supply fuel for the Bushehr reactor.

[22] *Implementation of the NPT Safeguards Agreement and Relevant Provisions of Security Council Resolutions in the Islamic Republic of Iran*, Report by the Director General, GOV/2010/62, November 23, 2010.

[23] Najmeh Bozorgmehrin, James Blitz, and Daniel Dombey, "Web Virus Aimed at Nuclear Work, Says Tehran," *Financial Times*, September 27, 2010.

[24] "Iran Official Points to West's Hand in Computer Worm at Nuclear Plant," *Islamic Republic of Iran News Network*, October 5, 2010.

[25] "Transmitting Virus to Iran Systems, In Vain- AEOI Chief," *Islamic Republic News Agency*, September 29, 2010.

[26] David Albright and Andrea Stricker, "Stuxnet Worm Targets Automated Systems for Frequency Converters: Are Iranian Centrifuges the Target?" Institute for Science and International Security, November 17, 2010.

components in the Bushehr reactor appears to be more likely because Siemens originally worked on the project.

Stuxnet's impact on Iran's nuclear facilities is unclear. Although, as noted, some Iranian officials have stated that the Bushehr reactor was not affected, some accounts suggest that the malicious software may have slowed down or disabled operations at Iran's enrichment facilities. For example, Iranian President Mahmoud Ahmadinejad said of the cyber attack that unnamed perpetrators "were able to cause minor problems with some of our centrifuges by installing some software in electronic parts. They did wrong. They misbehaved but fortunately, our experts discovered it."[27] Moreover, an unnamed "senior diplomat" suggested that Stuxnet may have caused Iran to shut down its commercial centrifuge facility for a few days in November 2010, Reuters reported November 23.[28]

Iranian officials have attributed the Stuxnet infections to a cyber attack, with some suggesting that Western countries are responsible. For example, Mahmoud Liaii characterized the worm as part of an "electronic war [that] has been launched against Iran."[29] Additionally, Mehmanparast suggested October 5 that the "West" is taking "steps and efforts to use every possible means to prevent the peaceful nuclear activities of our country."[30] An October 20 Open Source Center analysis, however, observed that Iranian officials have "largely remained vague" about Stuxnet's "target, intent, and origin."[31]

There have been previous allegations of efforts by the United States and other governments, including Israel, to sabotage Iran's centrifuge program. The *New York Times* reported in January 2009 that such efforts have included "undermin[ing] electrical systems, computer systems and other networks on which Iran relies," according to unnamed senior U.S. and foreign government officials.[32] One effort involved foreign intelligence services sabotaging "individual power units that Iran bought in Turkey" for Tehran's centrifuge program. "A number of centrifuges blew up," according to the *Times*.[33] Western governments have reportedly made other efforts to sabotage centrifuge components destined for Iran, according to some non-governmental experts.[34] Additionally, *New York Times* reporter James Risen wrote in 2006 that, according to unnamed U.S. officials, the United States engaged in a covert operation to provide Iran with flawed blueprints for a device designed to trigger a nuclear explosion.[35]

[27] "Wikileaks Revelations 'Worthless', 'Intelligence Game' - Iran President," *Islamic Republic of Iran News Network*, November 29, 2010.

[28] Fredrik Dahl and Sylvia Westall, "Technical Woes Halt Some Iran Nuclear Machines – Dips," *Reuters*, November 23, 2010.

[29] *Mehr News Agency*, September 25, 2010.

[30] *Islamic Republic of Iran News Network*, October 5, 2010.

[31] "Iran—Officials Characterize Stuxnet as 'Cyber War,' Maintain Ambiguity About Virus," *Open Source Center*, October 20, 2010.

[32] David E. Sanger, "U.S. Rejected Aid for Israeli Raid on Nuclear Site," *New York Times*, January 11, 2009.

[33] David E. Sanger and William J. Broad, "U.S. Sees an Opportunity to Press Iran on Nuclear Fuel," *New York Times*, January 3, 2010. Iranian officials alluded to this incident, according to a January 2007 Iranian press report (*Ayande-ye Now*, January 6, 2007).

[34] James Blitz, Roula Khalaf, and Daniel Dombey, "Suggestions of Iran Nuclear Sabotage," *Financial Times*, July 22, 2010.

[35] James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (New York: Free Press), 2006.

ICS Vulnerabilities and Critical Infrastructure

Vulnerabilities in industrial control systems have long been an issue of concern to both the security and technology communities.[36] Modern critical infrastructure facilities rely on computer hardware and software continuously to monitor and control equipment that supports numerous industrial processes, including nuclear plant management, electrical power generation, water distribution and waste control, oil and gas refinement, chemical production, and transportation management. The Department of Homeland Security (DHS) categorizes 18 critical infrastructure sectors as "essential to the nation's security, public health and safety, economic vitality, and way of life."[37] The advent of the Stuxnet virus has raised questions on the vulnerabilities of national critical infrastructure. In the absence of specific information on the full impact of Stuxnet, one can speculate that all these sectors may be at risk.

Many observers fear that a successful infiltration and attack could degrade or stop the operation of a critical infrastructure facility that delivers water, gas, or other essential utility, or affect multiple facilities due to the interdependent nature of the nation's infrastructure sectors responsible for providing essential services. Sean McGurk, the Department of Homeland Security's Acting Director of the National Cybersecurity and Communications Integration Center stated during a November 2010 hearing, "We have not seen this coordinated effort of information technology vulnerabilities and industrial control exploitation completely wrapped up in one unique package. To use a very overused term, it is a game-changer."[38] Unclassified reports suggest that the Stuxnet worm was specifically developed to seek out and exploit vulnerabilities in software that manages ICSs found in most critical infrastructure facilities. One type of ICS, a Supervisory Control and Data Acquisition (SCADA) system,[39] is a computer that controls industrial processes and infrastructures. SCADA systems can be accessed and managed directly at computer terminals, either from remote locations that are connected to the control system, or through the emerging trend of controlling these systems from mobile wireless devices.

In 2009, DHS conducted an experiment that revealed some of the vulnerabilities to cyber attack inherent in the SCADA systems that control power generators and grids. The experiment, known as the Aurora Project, simulated a computer-based attack on a power generator's control system that caused operations to cease.[40] The same vulnerabilities are said to exist in other critical infrastructure, which, if disabled, could both cripple the economy and have physical consequences; an electrical blackout for a prolonged period of time could potentially lead to loss of life if essential services were not restored. Yet some experts argue that the cyber threat to critical infrastructure is exaggerated, regardless of the perpetrators' capabilities.[41] For example,

[36] Guide to industrial control security, Department of Commerce, NIST, September 2008, http://csrc.nist.gov/publications/drafts/800-82/draft_sp800-82-fpd.pdf. See also Interview with Joseph Weiss, Cyberwar Frontline, Public Broadcasting Service, March 5, 2003, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/weiss.html.

[37] DHS website, Critical Infrastructure and Key Resources, http://www.dhs.gov/files/programs/gc_1189168948944.shtm, last accessed November 2, 2010.

[38] Rob Margetta, "Stuxnet Could Be a Harbinger of Threats to Come for U.S.," *Congressional Quarterly – Homeland Security*, November 17, 2010, http://homeland.cq.com/hs/display.do?docid=3764486&sourcetype=31&binderName=news-all.

[39] For more detailed information on SCADA, see http://www.ncs.gov/library/tech_bulletins/2004/tib_04-1.pdf.

[40] See "Challenges Remain in DHS' Efforts to Security Control Systems," Department of Homeland Security, Office of Inspector General, August 2009.

[41] Anthony H. Cordesman and Justin G. Cordesman, *Cyber-Threats, Information Warfare, and Critical Infrastructure* (continued...)

although the computer systems that control electricity plants could be penetrated by a sophisticated hacker, some infrastructure experts argue that the multitude of public and private companies and the overlapping nature of their operations creates a resiliency that would make long-term and widespread damage implausible.[42] Moreover, the North American power grid is segmented into four large regions, reducing the risk of a nation-wide failure. Yet due to their interconnected nature, it is possible that a failure in one system could cause cascading effects across an entire region. An example of this was seen in August 2003, when high-voltage power lines in Ohio came in contact with trees, triggering the automatic safety system to disconnect. Safety mechanisms of other generators then shut down and severed links between them, causing a blackout throughout the northeastern United States and Canada.[43]

Experts offer various recommendations to address the vulnerabilities described above. Some information security experts advocate mandatory encryption of computer data in SCADA-controlled utilities transmission and distribution systems. The Department of Energy is undertaking research and development efforts to modernize the electric grid with new information technology and thereby create a so-called "Smart Grid"[44] that will be more prevalent and accessible throughout the nation and may also be more secure. However, some security observers argue that creating a dependency on ubiquitous computer technologies will increase vulnerabilities to hacking, worms, viruses, or other cyber threats, and that a multi-layered, redundant network creates a higher level of protection.[45] Another option is to enhance the protection of the physical aspects of the nation's critical infrastructure, thus mitigating possible damage from a Stuxnet worm type of attack and also better preparing facilities to respond to natural or man-made threats.

National Security Implications

Whether it is electricity, telecommunications, transportation, or other essential services, many federal government activities rely on critical infrastructures that are predominately owned and operated by the private sector, which has an expectation of immediately accessible and fully operational use of these resources. Should the ICS of a critical infrastructure facility become affected by a Stuxnet worm or similar malicious code, disruptions could hamper the government's ability to provide domestic and international security, safety, and essential services for lengthy periods of time. Such an occurrence could also degrade the government's ability to pursue or maintain national security goals and thereby make the nation more vulnerable to a variety of foreign and domestic threats or contribute to a loss of public confidence in the government.

(...continued)

Protection: Defending the U.S. Homeland (Praeger Publishers, 2001), pp. 169-170.

[42] Seymour M. Hersh, "The Online Threat: Should we be worried about a cyber war?" *The New Yorker*, November 1, 2010.

[43] William D. O'Neil, "Cyberspace and Infrastructure," in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz (National Defense University Press, 2009).

[44] For more information about the Smart Grid, see the Department of Energy, The Smart Grid: An Introduction, http://www.oe.energy.gov/SmartGridIntroduction.htm. For further information, see The Smart Grid: An Introduction prepared for the U.S. Department of Energy by Litos Strategic Communication, 2008, accessed at http://www.oe.energy.gov/DocumentsandMedia/DOE_SG_Book_Single_Pages(1).pdf.

[45] See 21 Steps to Improve Cyber Security of SCADA Networks, U.S. Department of Energy, accessed at http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf.

The predominant view of many security observers appears to be that the recent emergence of the worm may be a new type of threat that could potentially lead to short- and long-term adverse global security consequences. However, some security experts claim that the threat of cyberwar in general is exaggerated by security firms and government entities in an effort to procure more resources and control over information technology.[46] Yet these claims are not related specifically to Stuxnet. In October 2010, Dr. Udo Helmbrecht, Executive Director of the European Network and Information Security Agency, stated, "Stuxnet is really a paradigm shift, as Stuxnet is a new class and dimension of malware. Not only for its complexity and sophistication ... the fact that perpetrators activated such an attack tool can be considered as the 'first strike,' i.e. one of the first organized, well prepared attack against major industrial resources. This has tremendous effect on how to protect national (critical infrastructure) in the future."[47] The Stuxnet worm is unique because the software code appears to have been designed to infiltrate and attack an ICS often used by critical infrastructure facilities in order to cause long-term physical damage to them. Although the full extent of damage caused by Stuxnet is unknown, the potential implications of such a capability are numerous in that the worm's ability to identify specific ICSs and wait for an opportune time to launch an attack could have catastrophic consequences on nations' critical infrastructures.

Issues

The possibility of this type of cyber threat to national critical infrastructure raises several questions for policymakers. It is said that actions in cyberspace are conducted in milliseconds. When the consequences of retaliatory actions in cyberspace may be unknown, is an immediate response required, or a longer, more deliberative process? The lack of clear attribution further complicates the issue. If a cyber attack appeared to be launched from an unsuspecting neutral country, it may not be possible to formally engage that country in stopping an attack that is taking place in milliseconds. What authorities should be in place if such an attack were deemed to warrant an immediate response from the affected nation? Is an international treaty or convention necessary to curb proliferation and use of cyber-based weapons? Many arms control treaties are built upon inspection, verification, and compliance regimes. As nefarious activities in cyberspace defy geographical boundaries and often attribution, how would such activities be conducted in a cyber arms control treaty?

Another issue raised by Stuxnet is the government's role in protecting critical infrastructure. Is the Department of Homeland Security equipped to protect national infrastructure? Would new authorities be necessary in order to oversee the defense of privately owned critical infrastructure facilities? What is the military's role in defending national critical infrastructure from cyber attack? What role should intelligence agencies have in monitoring private infrastructure? Is the threat of cyber war exaggerated in order to shift power over the internet to the military and intelligence agencies? Is the private sector the first line of defense in the event of a cyber attack on critical infrastructure? Is new legislation required to standardize and regulate critical infrastructure protection throughout the various sectors?

[46] Ryan Singel, "Cyberwar Hype Intended to Destroy the Open Internet," *Wired*, March 1, 2010.

[47] EU Agency analysis of 'Stuxnet' malware: a paradigm shift in threats and Critical Information Infrastructure Protection, Press Release initial comment and brief, high level analysis of the recent 'Stuxnet' attacks, October 7, 2010, http://www.enisa.europa.eu/media/press-releases/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1.

Appendix. Glossary

Malware Malware is a general term used to describe various types of malicious software.

Worm A worm is a type of malware that can copy itself and spread through a network, without attaching itself to a file.

Virus A virus usually refers to a computer program that can infect a file, copy itself, and spread to other computers.

Botnet A botnet is a collection of malware-infected computers that are controlled by a remote source.

ICS The term ICS encompasses software that controls production and distribution in industries such as oil, water, electrical, gas, and data.

IP Internet Protocol is the language and method by which data is transmitted between computers. An IP address is a computer's numerical assignment.

Code The numbers, letters, and symbols used to deliver instructions to a computer. A computer program is composed of code.

Server A server is a computer or program that provides services to other computers.

Air-gapped An air-gapped network is one that is not connected to any other network, including the Internet, and only allows internal data transmission.

Author Contact Information

Paul K. Kerr
Analyst in Nonproliferation
pkerr@crs.loc.gov, 7-8693

John Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529

Catherine A. Theohary
Analyst in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844