SSI STRATEGIC STUDIES INSTITUTE

Executive Summary

Strategic Studies Institute and U.S. Army War College Press

UNITED STATES ARMY WAR COLLEGE PRESS
Carlisle Barracks, PA STRENGTH and WISDOM

CYBERTERRORISM AFTER STUXNET

Thomas M. Chen

Public government statements have cited concerns that terrorists might be turning to cyber attacks. In theory, terrorists of sufficient skills might be able to attack a wide range of critical targets such as the power grid, air traffic, public transport, and communication networks, potentially causing large-scale devastation. However, no major cyber terrorist attacks have been observed to date, raising doubts about the reality of the threat.

Stuxnet was a recent milestone in the arena of cyber security because, although a cyber attack on industrial control systems was long believed to be theoretically possible, it was different to see malware used in reality as a weapon against an enemy's infrastructure. Stuxnet was clearly designed for real-world damage (sabotage) to industrial control systems. Stuxnet's payload is too specific to worry about its reuse by terrorists, but it does raise a concern that a sufficiently determined adversary might be able to cause physical damage to the U.S. critical infrastructure through a cyber attack. Terrorists now know that cyber attacks are not limited to computers, and investment in cyber attacks can actually pay off in real-world damage.

This monograph asks if Stuxnet has had an effect on cyber terrorism in terms of motive, means, and opportunity. Are terrorists interested in launching cyber attacks against U.S. critical infrastructures? Are terrorists building capabilities and skills for cyber attacks? How vulnerable are U.S. critical infrastructures?

Terrorist Motives and Interest.

The cyber domain offers several benefits to achieve terrorists' main aim to gain visibility and influence by creating fear through "breaking things and killing people": anonymity, relative safety, low cost, availability of cyber attack tools, low skill requirement, and remote access to vulnerable targets. The interest of terrorists in cyber attacks have been evident in many online forums set up to distribute manuals and tools for hacking, and to promote and coordinate cyber attacks (sometimes called "electronic jihad"). Al-Qaeda has long supported electronic jihad, particularly as a means of disrupting the U.S. economy, and al-Qaeda prisoners have told interrogators about their intent to use cyber attack tools. In late-2010, the popular Al-Shamukh jihadist forum called for attacks on industrial control systems, noting the success of Stuxnet.

Terrorist Cyber Capabilities.

Terrorists have been active online but not at a level of sophistication comparable to Stuxnet. Stuxnet was developed by military expert programmers with detailed knowledge about their target. It would take enormous time and human resources to develop that level of sophisticated skills. In addition to information technology (IT) skills, an important element of major cyber attacks is zero-day exploits, as used in Stuxnet. It might be assumed that terrorists might easily be able to buy zero-day exploits as needed. However, there is also competition from many Western companies and organizations, so terrorists may find it difficult to acquire zero-day exploits. Instead of developing their own skills and attack tools, terrorists might find it easier to pay third parties to carry out attacks for them. Indeed, cybercrime or hacker groups might be hired, but this approach is unlikely because it would be far more costly than traditional physical attacks that terrorists have used more or less successfully in the past.

Opportunity.

It is well known that about 90 percent of U.S. critical infrastructure is privately owned, and cyber security tends to be a low priority. The number of vulnerabilities appears to be increasing rapidly. Another vulnerability is the complexity and high connectedness of systems, which increases the risk of cascade failures.

Since we have established motive, means, and opportunity for terrorists, the natural question is why a major cyber attack has not happened yet? It seems that al-Qaeda and other terrorist groups still prefer bombs and physical attacks, even after Stuxnet. In 2007, Professor Dorothy Denning postulated three indicators that could precede a successful cyber terrorism attack, and so far, none of these indicators have been observed. This would imply that terrorists are not trying hard to prepare for cyber attacks.

Perhaps the most straightforward explanation of the lack of observed cyber attacks is the cost-benefit argument put forth by Giampiero Giacomello. He compared the costs of traditional physical terrorist attacks with cyber attacks of the "break things and kill people" type, and concluded that bombs are a much cheaper approach than cyber attacks by orders of magnitude. Stuxnet, estimated to have cost millions of dollars, does not change the cost-benefit comparison. Even after Stuxnet, terrorists still face a considerable cost barrier to carrying out large-scale cyber attacks. Therefore, cyber attacks are probably unlikely in the near future.

However, the cost-benefit argument does not completely rule out the possibility of cyber attacks as a means of complementing physical attacks. In that case, the cyber attacks could be much more modest, not necessarily of the "break things and kill people" type. In addition, it is quite possible that development costs for Stuxnet-like malware could decrease in the future. If that happens, the cost-benefit argument could predict a point in the future when cyber attacks could become attractive for terrorists.

It seems little can be done to change motive for terrorists. Some analysts have proposed the idea of deterrence, but it is questionable whether deterrence is feasible in the cyber domain. Also, it seems that little can be done to change means for terrorists. Although terrorists do not have a high level of cybercapabilities yet, it would be practically difficult to prevent them from acquiring skills or help from third parties. The only factor that is feasible to address is opportunity. Specifically, policies should enhance protection of national infrastructures to reduce the risk exposure to cyber attacks. Fortunately, the U.S. Government has already placed top priority on vulnerabilities in critical infrastructures.

All measures to reduce the opportunity for cyber terrorists are recommended. However, the adaptiveness and resourcefulness of terrorists should not be underestimated. It will be practically impossible to fix every vulnerability. Perhaps policies should recognize that cyber attacks will be inevitable, and instead address the cost-benefit proposition for terrorists. If systems can be designed to increase costs and reduce benefits to adversaries, attacks will become less appealing.

*****

More information about the programs of the Strategic Studies Institute (SSI) and U.S. Army War College (USAWC) Press may be found on the Institute's homepage at *www.StrategicStudiesInstitute.army.mil.*

*****

This Publication SSI Website USAWC Website