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

# CYBERTERRORISM AFTER STUXNET

Thomas M. Chen

U.S. ARMY WAR COLLEGE
SSI
STRATEGIC STUDIES INSTITUTE

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

# The United States Army War College

The United States Army War College educates and develops leaders for service at the strategic level while advancing knowledge in the global application of Landpower.

The purpose of the United States Army War College is to produce graduates who are skilled critical thinkers and complex problem solvers. Concurrently, it is our duty to the U.S. Army to also act as a "think factory" for commanders and civilian leaders at the strategic level worldwide and routinely engage in discourse and debate concerning the role of ground forces in achieving national security objectives.

SSI
STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute publishes national security and strategic research and analysis to influence policy debate and bridge the gap between military and academia.

CSLD
CENTER for STRATEGIC LEADERSHIP and DEVELOPMENT
U.S. ARMY WAR COLLEGE

The Center for Strategic Leadership and Development contributes to the education of world class senior leaders, develops expert knowledge, and provides solutions to strategic Army issues affecting the national security community.

PKSOI

The Peacekeeping and Stability Operations Institute provides subject matter expertise, technical review, and writing expertise to agencies that develop stability operations concepts and doctrines.

U.S. Army War College
SLDR
Senior Leader Development and Resiliency

The Senior Leader Development and Resiliency program supports the United States Army War College's lines of effort to educate strategic leaders and provide well-being education and support by developing self-awareness through leader feedback and leader resiliency.

SCHOOL OF STRATEGIC LANDPOWER
U.S. Army War College

The School of Strategic Landpower develops strategic leaders by providing a strong foundation of wisdom grounded in mastery of the profession of arms, and by serving as a crucible for educating future leaders in the analysis, evaluation, and refinement of professional expertise in war, strategy, operations, national security, resource management, and responsible command.

The U.S. Army Heritage and Education Center acquires, conserves, and exhibits historical materials for use to support the U.S. Army, educate an international audience, and honor Soldiers—past and present.

# STRATEGIC STUDIES INSTITUTE

The Strategic Studies Institute (SSI) is part of the U.S. Army War College and is the strategic-level study agent for issues related to national security and military strategy with emphasis on geostrategic analysis.

The mission of SSI is to use independent analysis to conduct strategic studies that develop policy recommendations on:

- Strategy, planning, and policy for joint and combined employment of military forces;
- Regional strategic appraisals;
- The nature of land warfare;
- Matters affecting the Army's future;
- The concepts, philosophy, and theory of strategy; and,
- Other issues of importance to the leadership of the Army.

Studies produced by civilian and military analysts concern topics having strategic implications for the Army, the Department of Defense, and the larger national security community.

In addition to its studies, SSI publishes special reports on topics of special or immediate interest. These include edited proceedings of conferences and topically oriented roundtables, expanded trip reports, and quick-reaction responses to senior Army leaders.

The Institute provides a valuable analytical capability within the Army to address strategic and other issues in support of Army participation in national security policy formulation.

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

# CYBERTERRORISM AFTER STUXNET

**Thomas M. Chen**

**June 2014**

*****

Comments pertaining to this report are invited and should be forwarded to: Director, Strategic Studies Institute and U.S. Army War College Press, U.S. Army War College, 47 Ashburn Drive, Carlisle, PA 17013-5010.

*****

This manuscript was funded by the U.S. Army War College External Research Associates Program. Information on this program is available on our website, *www.StrategicStudies Institute.army.mil*, at the Opportunities tab.

*****



*****

The Strategic Studies Institute and U.S. Army War College Press publishes a monthly email newsletter to update the national security community on the research of our analysts, recent and forthcoming publications, and upcoming conferences sponsored by the Institute. Each newsletter also provides a strategic commentary by one of our research analysts. If you are interested in receiving this newsletter, please subscribe on the SSI website at *www.StrategicStudiesInstitute.army.mil/newsletter.*

ISBN 1-58487-627-1

## FOREWORD

Public government statements have cited cyber-attacks by terrorists as a major concern for national security. To date, no large-scale cyber-terrorist attack has been observed, but terrorists are known to be using the Internet for various routine purposes. The discovery of Stuxnet in 2010 was a milestone in the arena of cybersecurity because, although a malware attack on industrial control systems was long believed to be theoretically possible, it was different to see malware used in reality to cause real physical damage. Stuxnet demonstrated that a sufficiently determined adversary with sufficient resources might be able to damage U.S. critical infrastructure physically through a cyber attack. Did Stuxnet change the threat of cyber-terrorism?

This monograph examines cyberterrorism before and after Stuxnet by addressing three questions: 1) Motive—Are terrorists interested in launching cyber-attacks against U.S. critical infrastructures? 2) Means—Are terrorists building capabilities and skills for cyberattacks? and, 3) Opportunity—How vulnerable are U.S. critical infrastructures? Answers to these questions give a characterization of the post-Stuxnet cyberterrorism threat. The next question is why a major cyber-terrorist attack has not happened yet; this is explained from a cost-benefit perspective. Although cyberterrorism may not be an imminent threat, there are reasons to be concerned about the long-term threat and inevitability of cyberattacks.

It is important to assess frequently the threat landscape and current government policies for enhancing the protection of national infrastructures.

Therefore, the Strategic Studies Institute commends this monograph to its readers.

DOUGLAS C. LOVELACE, JR.
Director
Strategic Studies Institute and
U.S. Army War College Press

## ABOUT THE AUTHOR

THOMAS M. CHEN is a professor of cybersecurity in the School of Engineering and Mathematical Sciences at City University London, United Kingdom (UK). He was formerly a Professor in Networks in the College of Engineering at Swansea University, UK. Prior to joining Swansea University, he was an Associate Professor in electrical engineering at Southern Methodist University, Dallas, Texas, and a senior member of technical staff at GTE R&D Laboratories (now Verizon Labs), Waltham, Massachusetts. He has 22 years of research experience in academia and industry. Dr. Chen has published widely on issues related to Internet security. His work has been supported by government agencies, such as the National Science Foundation and Department of Homeland Security, and various companies including Nortel Networks, Alcatel, and Sprint. He regularly collaborates with researchers in major security companies. Recently he has been involved in an interdisciplinary research project in cyberterrorism with colleagues in Law and Political Science at Swansea University. Dr. Chen holds B.S. and M.S. degrees from Massachusetts Institute of Technology, and a Ph.D. in electrical engineering from University of California, Berkeley.

## SUMMARY

Terrorists are known to use the Internet for communications, planning, recruitment, propaganda, and reconnaissance. They have shown interest in carrying out cyberattacks on U.S. critical infrastructures, although no such serious attacks are known publicly to have occurred. The discovery of the Stuxnet malware in July 2010, and its analysis over the next several months, was widely believed to have been a landmark event in cybersecurity, because it showed that cyberattacks against industrial control systems, hypothesized for a long time, are actually possible. After Stuxnet, there were public concerns that terrorists might be encouraged to acquire capabilities for similar cyberattacks.

This monograph examines cyberterrorism before and after Stuxnet by addressing questions of:

1. Motive—Are terrorists interested in launching cyberattacks against U.S. critical infrastructures?
2. Means—Are terrorists building capabilities and skills for cyberattacks?
3. Opportunity—How vulnerable are U.S. critical infrastructures?

It is noted that no serious cyberterrorism attacks have occurred after Stuxnet. This can be explained from a cost-benefit perspective that has not changed since Stuxnet. It can be argued that U.S. policies can really address vulnerabilities only by strengthening defenses of critical infrastructures.

# CYBERTERRORISM AFTER STUXNET

## INTRODUCTION

There have been widely publicized government concerns that terrorists might be turning to cyberattacks. For instance, Federal Bureau of Investigation (FBI) Director Robert Mueller testified to a Senate Appropriations Subcommittee in March 2012 that "while to date terrorists have not used the Internet to launch a full-scale cyber attack, we cannot underestimate their intent. . . . (terrorists are) using cyberspace to conduct operations."[1] Cited examples of terrorist "cybersavvy" included al-Qaeda in the Arabian Peninsula, which publishes an online magazine entitled *Inspire*, and the use of Twitter by the Somali group Al-Shabaab. The prospect of cyberterrorism is understandably troubling, because of the wide range of possible targets and attack vectors, which would be challenging in terms of defense. In theory, terrorists of sufficient skills might be able to attack the power grid, air traffic, public transport, financial networks, communication networks, emergency response, utilities, manufacturing plants, or military networks. Possible cyberattacks could range from blatant distributed denial of service (DDoS) or sabotage, to more stealthy attacks for data theft or remote control.

According to Gabriel Weimann, "psychological, political, and economic forces have combined to promote the fear of cyber terrorism."[2] The concept combines two modern psychological fears: the fear of random violence and the fear of computer technology. Also, cyberterrorism has been caught up in the U.S. political aftermath of September 11, 2001 (9/11), when more terrorist attacks seemed to be a distinct possibil-

ity, and the United States felt vulnerable. The prospect of cyberattacks causing catastrophic damage from a remote computer seemed like the ultimate threat, perhaps hyped beyond the actual threat level. Weimann states that a threat is real but must be assessed realistically without overdue emotional influences.

The first obstacle in assessing cyberterrorism are the various definitions that have been proposed. No single definition has been universally accepted (just as a common definition of terrorism has been elusive). The term might be traced back originally to Barry Collin,[3] who noted that physical infrastructures increasingly are controlled by computers, and that dependence on computer networks increased our vulnerability to cyberattacks. Examples of potential targets for cyberattacks included: financial systems to disrupt stock exchanges; air-traffic control to crash aircraft; pressure valves in gas lines to cause explosions; and computer controls at pharmacies or food processing plants to poison the population. Like traditional terrorist acts, cyberterrorism exhibits scale (mass destruction) and publicity. Collin postulated that cyberattacks would appeal logically to terrorists for their relative ease and safety. At the same time, Collin predicted that cyberterrorism would create new challenges to counter terrorism because of the need to acquire cyber expertise and eliminate vulnerabilities in critical infrastructures.

Professor Dorothy Denning offered a definition of "cyberterrorism" in testimony before the House Armed Services Committee in May 2000 that has been widely cited:

> Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, net-

> works and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.[4]

A more concise definition is "politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage."[5] This definition consists of three parts: 1) politically driven intention; 2) serious effects; and, 3) computer networks as the means. This meaning shares commonalities with the U.S. Department of State definition of terrorism in Title 22 of the U.S. Code, Section 2656f(d): "Premeditated politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience."[6]

Generally, Denning's definition of cyberterrorism is the one used here. Definitions are problematic, because complicated scenarios could be imagined. For example, a physical attack on computers controlling critical infrastructures could cause serious harm; in this case, computers are the target but not the means. Also, terrorists use computer networks for recruiting, planning, communications, and target reconnaissance. These are routine activities that most people use the Internet for, but might be argued to be cyberterrorism in the sense of "cyber activities supporting terrorism."

Aside from the problem of definition, there is the practical problem of determining whether a particular cyberattack qualifies as cyberterrorism.[7] First, attribution of cyberattacks to the real attacker is difficult and often impossible. Attackers can compromise other computers to use as intermediaries, or channel through anonymizing proxies that hide their Internet protocol (IP) address. Second, the complete effects of an attack might be concealed, e.g., if stealthy malware has been installed without detection. Third, even if attribution is solved, there is another problem: determining the intent of the attacker. For instance, it would be difficult to determine if a hacking group is acting for its own gain or was hired by another party.

Aside from definitions, the cyberterrorism literature has addressed mostly: 1) how terrorists use the Internet for propaganda, recruiting, fund raising, intelligence gathering, and planning; 2) vulnerabilities in critical infrastructures, providing opportunities for cyberattacks; and, 3) whether cyberterrorism is a real threat. Most of the literature understandably predates Stuxnet, since the discovery of Stuxnet was relatively recent. Stuxnet vividly demonstrated to the world that industrial systems can be sabotaged physically by malware, a threat long believed to be possible by the cybersecurity community but not actually observed. The literature has not really explored whether Stuxnet had any effect on cyberterrorism.

This monograph examines cyberterrorism before and after Stuxnet by addressing these questions: 1) Motive—Are terrorists interested in launching cyberattacks against U.S. critical infrastructures? 2) Means—Are terrorists building capabilities and skills for cyberattacks? and, 3) Opportunity—How vulnerable are U.S. critical infrastructures? It is noted that no serious cyberterrorism attacks have occurred af-

ter Stuxnet; this can be explained from a cost-benefit perspective, which has not changed since Stuxnet. In that sense, cyberterrorist attacks do not seem to be imminent, although Stuxnet has implications for the cost-benefit weights of potential future attacks. It can be argued that U.S. policies can really address only the opportunities for terrorism (but not motive or means) by strengthening the defenses of critical infrastructures.

## STUXNET

Stuxnet was a milestone in the field of cyber scecurity. Although experts had long believed that a malware attack on industrial control systems was possible, it was different to see it used in reality as a surgical strike against an enemy's infrastructure. Stuxnet revealed the level of sophistication required for a "weaponized" malware.

The unusual size and sophistication of Stuxnet, discovered in June 2010, took a team of antivirus companies several months to diagnose its functions fully. Today, Stuxnet is well understood[8] and documented[9] but still surprising in the level of effort invested by the terrorists and its technical sophistication. The description of Stuxnet here is summarized from the literature.

Stuxnet stood out from typical malware due to its large size (around 500 kilobytes [kb]) and complexity. It was unusual in that it used two stolen digital certificates and multiple zero-day exploits. As zero-day exploits are valuable, typical malware usually contains at most one zero-day (or often none, as reused known exploits can still be effective against unpatched targets). The level of investment suggests that the target was considered very valuable, but it took months to analyze the payload and ascertain the probable target.

**Methods of Spreading.**

The initial infection vector was suspected to be a removable drive because the target network was not connected to the Internet. Once a personal computer (PC) has been infected, Stuxnet uses various means to spread through local networks to other PCs:

- Stuxnet detects the presence of removable drives (probably a universal serial bus [USB] flash) and installs several files for infecting a Windows PC, exploiting a vulnerability in the processing of shortcuts and .lnk files (MS10-046). When the infected drive is opened in a PC, Stuxnet's binaries will be executed.
- Stuxnet exploits a vulnerability in the Windows Print Spooler service to spread by sending a malicious print request to a target PC over a remote procedure call (RPC).
- Stuxnet exploits an old vulnerability in Windows Server Service (MS08 067) which does not properly handle specially crafted RPC requests.
- Stuxnet spreads to other PCs through network shares.
- Stuxnet takes advantage of a hard-coded default password in Siemens Simatic WinCC software (CVE-2010-2772). The password allows privileged access to a back-end WinCC database. Once connected to the database, Stuxnet injects a copy of itself into the database, thereby infecting the PC running the WinCC database.

**Target.**

While Stuxnet is capable of spreading more aggressively, it is interested only in Windows PCs running Simatic Step 7 software, because the ultimate target was a Siemens Simatic S7 PLC (programmable logic controller). Stuxnet contains code to test that the target is correct. Also, the analysis of the payload pointed to a Siemens Simatic S7 PLC target. PLCs are specialized computers used widely to control various types of industrial equipment found in factories, assembly lines, manufacturing plants, and critical infrastructures.[10] Like PCs, PLCs are programmable for flexibility but differ in a few important respects: they are for more rugged environments and for specific real-time applications; they are not connected to the Internet or wide-area networks; and, they are typically equipped with more elaborate input/output interfaces than PCs. PLCs are commonly connected to a programming device—usually a regular PC—and disconnected after a program is loaded.

Stuxnet is interested only in Siemens Simatic S7 PLCs, which are programmed by Windows PCs running Simatic Step 7 software.[11] After Stuxnet infects a PC running Simatic Step 7, Stuxnet will then load its own malicious blocks into a connected Simatic S7 PLC. The malicious blocks are capable of hiding their presence from the human operator. Stuxnet also checks the type of central processing unit (CPU) in the PLC, the presence of Profibus (a standard industrial network bus), and the presence of at least 33 frequency converter drives made by Fararo Paya (Iran) or Vacon (Finland). The reason is that the payload evidently is aimed at affecting these specific frequency converter drives. The creators of Stuxnet had knowledge that

the intended target PLCs would have these frequency converter drives.

**Payload.**

Stuxnet chooses one of three infection sequences for delivering the payload, depending on the configuration of the Siemens Simatic S7 PLC. In actuality, the first two sequences are similar, while the third sequence is disabled; hence, there is essentially one infection sequence and one payload. The payload gives Stuxnet the capability to modify data to and from the connected frequency converter drives. By modifying the data, Stuxnet can alter the operating frequencies of the drives to make them fail over time. According to later reports, the target was Iran's Natanz uranium enrichment plant; the sabotage was deliberately subtle so that the human operators would be mystified about the cause.[12]

According to the control systems security firm Langner Communications, the payload in Stuxnet also attempts to disrupt turbine control systems. If this theory is valid, it would suggest that Stuxnet could have been created for Iran's Bushehr nuclear power plant as well as the Natanz uranium-enrichment plant. The payload modules aimed at the turbine control systems at Bushehr appear to carry out a man-in-the-middle attack in order to pass fake input and output values to the genuine plant control code, presumably to disrupt the turbine control systems.

**Significance and Implication.**

Most malware is intended for computer systems (e.g., stealing data, establishing backdoors), but Stuxnet was clearly designed for real-world damage (sabo-

tage) of industrial control systems. Moreover, it was crafted deliberately to deliver a payload to a specific high-value target. Stuxnet is too specific to worry about its reuse by terrorists. Even if terrorists acquired a copy of the source code, it would take an enormous amount of effort to re-engineer a different payload. Most likely different exploits would be needed because the exploits used by Stuxnet have mostly been patched since its discovery.

More worrisome is that Stuxnet demonstrates that a sufficiently determined adversary with sufficient resources might be able to damage U.S. critical infrastructure physically through a cyberattack. The level of effort to create Stuxnet has been estimated to cost millions of dollars, so the required resources would be very substantial. However, that cost is not beyond the budget of large terrorist organizations. Terrorists do not have to invest in creating their own custom-built malware, but eventually will be able to buy attack tools from criminal organizations or friendly nations. Stuxnet has gotten the attention of the world by promoting an arms race to develop offensive (and defensive) cybercapabilities among nations and the underground.

In summary, Stuxnet changed a theoretical hypothesis into reality; terrorists now know that cyberattacks are not limited to computers, and investment in cyberattacks can actually pay off in real-world "breaking things and killing people." There is more likely to be a long-term affect than a short-term one. The following sections ask if Stuxnet has had an effect in terms of motive, means, and opportunity for terrorists.

## TERRORIST MOTIVES AND INTEREST IN CYBER ATTACKS

There are many logical reasons to expect terrorists to be interested in cyberterrorism.[13] First, consider their motivations. Their main aim is clearly to gain visibility and influence by creating fear through "breaking things and killing people."[14] Lesser goals are to maintain their operations and carry out their activities, e.g., fund raising, planning, recruitment, and intelligence gathering. The cyber domain offers several benefits to achieve those aims:

- Anonymous communications with other terrorists;
- Personal safety compared to physical attacks (e.g., bombs, suicide missions);
- Easy access to online data about potential targets;
- Low cost (PC or smart phone);
- Availability of abundance of cyber attack tools;
- Low skill entry: many attack tools are automated, needing little expertise;
- Remote access to vulnerable targets;
- Reachability to any network-connected target;
- Connection to a worldwide audience for propaganda;
- Asymmetry: small terrorist groups can carry out large-scale attacks.

### Terrorist Uses of the Internet.

It has been well documented that terrorists are knowledgeable about computers and use the Internet regularly for various activities supporting terrorism,

such as propaganda, recruiting, communications, planning, and intelligence gathering.[15] A recent United Nations (UN) Office on Drugs and Crime report[16] found that terrorists use the Internet to:

- Spread propaganda related to instruction, explanations, justifications, or promotion of terrorist activities;
- Incite violence;
- Recruit and radicalize individuals;
- Raise funds through direct solicitation, e-commerce, the exploitation of online payment tools, and through charitable organizations;
- Train followers for combat tactics, the use of explosives and of weapons;
- Plan and coordinate attacks, often involving covert communication among several parties.

Internet usage has increased with changes in terrorist organizations. In the past, terrorist groups have been mostly hierarchical, which is a more effective structure for carrying out tasks and missions. More recently, terrorist groups such as al-Qaeda and Hamas have been organized as loosely interconnected, semi-independent cells without a single commanding hierarchy, for resilience against disruption or capture. The Internet is vital for facilitating communications and coordination among loosely interconnected groups.

Denning pointed out that it is not simply that terrorists are using the Internet, but more significantly, that the Internet has transformed the current practice of terrorism.[17] For instance, most terrorist groups now have a Web presence. Al-Qaeda has been using the Web since the late-1990s, initially through the website, *alneda.com*. Today al-Qaeda has thousands of websites. Jihadist websites are used to distribute a wide variety

of materials such as the writings and recordings of Osama bin Laden, Ayman al-Zawahiri, and other al-Qaeda leaders; videos of bombings and other terrorist acts; fatwas (religious edicts); electronic magazines; training manuals and videos; news reports; calls to join the jihad; and software tools. Al-Qaeda's online training materials have evidently been useful for planning attacks. Reportedly, the principal architect of the 9/11 attacks, Khalid Shaikh Mohammed, trained high-level al-Qaeda operatives in the use of encryption (terrorists have been captured with encrypted files on their computers).

Besides the Web, terrorists have established groups on social networking sites. Marc Sageman (author of *Leaderless Jihad*) has noted that websites are used primarily for distributing materials and propaganda, but it is through interactive forums and chat rooms that relationships are built and personal bonding takes place. Individuals are drawn online with little risk or cost, from anywhere in the world. They can support terrorism without necessarily having to acquire or handle explosives or anything directly harmful to people.

In November 2003, the Saudi-owned London daily *Al-Shrq al-Awsat* reported that al-Qaeda had opened a virtual university on the Internet called al-Qaeda University for Jihad Sciences. It includes colleges for technologies related to explosive devices and to electronic and media jihad.

**Interest in Cyberattacks.**

Terrorists have been active online but not at a level of sophistication comparable to that of Stuxnet. Perhaps one of the first reported incidents was in 1997.

A group called Internet Black Tigers, aligned with the Liberation Tigers of Tamil Eelam (LTTE), claimed responsibility for "suicide email bombings" against Sri Lankan embassies over a 2-week period. The cyberattacks consisted of disk-operating systems and Web defacements.

Many forums have sprung up to distribute manuals and tools for hacking, and to promote and coordinate cyberattacks (sometimes called "electronic jihad"). Sites such as *7hj.7hj.com* teach surfers the art of computer attacks and trains individuals in hacking skills to serve Islam. A 2006 report by the Jamestown Foundation reported that most radical jihadi forums devote an entire section to hacking.[18] For example, it reported that the al-Ghorabaa site published information about how to penetrate computer devices and intranet servers and steal passwords,[19] including a 344-page book on hacking techniques.[20]

Al-Qaeda has long supported "electronic jihad," particularly as a means of disrupting the U.S. economy. While truck bombs could accomplish a great deal of physical damage, there would not be much damage to the U.S. economy. On the other hand, a cyberattack might have a chance to take down the entire financial services network. Muhammad bin Ahmad as-Salim, in a book entitled *39 Ways to Serve and Participate in Jihad*, encourages the use of electronic jihad as one of the ways to support al-Qaeda. In another book entitled *al-Zarqawi – al-Qaeda's Second Generation*, journalist Fouad Hussein describes a seven-phase war by al-Qaeda in which the organization plans to take over the world and turn it into an Islamic state.[21]

Phase 1 consisted of raising the consciousness of Muslims worldwide after the 9/11 attacks. Phase 4, spanning 2010 to 2013, included cyberterrorism to damage the U.S. economy.

After 9/11, Osama bin Laden was quoted by the Pakistani newspaper *Ausaf* as saying:

> Hundreds of young men had pledged to him that they were ready to die and that hundreds of Muslim scientists were with him and who would use their knowledge in chemistry, biology and ranging from computers to electronics against the infidels.[22]

This suggested that bin Laden had some capabilities of launching cyberattacks. Al-Qaeda prisoners have told interrogators about their intent to use cyberattack tools, and captured al-Qaeda computers have been found to contain schematics and software for simulating catastrophic scenarios of a dam.[23] Al-Qaeda computers have also reportedly contained evidence of surveillance of nuclear power plants, dams, and other critical infrastructures.[24] Lamar Smith, a Representative from Texas, reported that Congress has been briefed on al-Qaeda operatives probing the electronic infrastructure in search of ways to disrupt or disable power, phones, and water supplies. Smith claimed, "There is a 50 percent chance that the next time al Qaeda terrorists strike the United States, their attack will include a cyberattack."[25]

Has Stuxnet increased terrorist interest in cyberattacks on U.S. critical infrastructure? In late-2010, the popular Al-Shamukh jihadist forum called for attacks on industrial control systems, noting the success of Stuxnet. The Forum posted a broad overview of supervisory control and data acquisition (SCADA) systems, but not information on how to attack them. Congressional testimony after Stuxnet raised concerns about the damage caused by a potential Stuxnet-like attack, but no testimony warned of any imminent attack or change in the capabilities of terrorists.[26] Thus, it seems

that Stuxnet might have raised awareness but did not significantly change the intent or interest of terrorists.

## TERRORIST CAPABILITIES

Having established that terrorists are interested in cyberattacks, the next question is whether terrorists are building up capabilities and skills for such cyberattacks. There seems little doubt about their intentions, although their skill levels currently are not nearly comparable to the level of Stuxnet. In March 2010, testimony, FBI Director Mueller stated:

> We in the FBI, with our partners in the intelligence community, believe the cyber terrorism threat is real, and it is rapidly expanding. Terrorists have shown a clear interest in pursuing hacking skills. And they will either train their own recruits or hire outsiders, with an eye toward combining physical attacks with cyber attacks.[27]

It is true that a multitude of easy-to-use software attack tools are readily available at no or low cost. For a small investment, attacks such as DDoS can be waged with serious and costly impact. It is also true that Islamic fundamentalist organizations such as Hamas, al-Qaeda, Algeria's Armed Islamic Group, Hezbollah, and the Egyptian Islamic Group are known to be versed in information technology. However, the type of attacks that are possible with low-cost tools do not yet rise anywhere near the level of "breaking things and killing people." It is very unlikely that any terrorist organization such as al-Qaeda will be able to deploy a cyberattack with the sophistication of Stuxnet. Stuxnet was developed by military expert programmers with detailed knowledge about their

targets. It would take enormous time and human resources to develop that level of sophisticated skills. Although terrorists might turn to the underground to hire hackers with sufficient skills, Giampiero Giacomello has argued that 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.[28]

In addition to IT skills, an important element of major cyberattacks is zero-day exploits (as used in Stuxnet), because no patch is available to defend against them. There is a thriving market for zero-day exploits, and it might be assumed that terrorists might be able to buy them easily as needed. However, there is also competition. At the recent Black Hat conference, representatives from the U.S. military and intelligence community were among the thousands of attendees to learn about vulnerabilities and buy exploits and software tools, among other things. Many of the companies involved in discovering vulnerabilities and creating exploits are in Western countries unfriendly to terrorists, so terrorists may find it very difficult to acquire zero-day exploits.

Denning described a model for assessing cyberterror capability that consisted of three levels:[29]

1. Simple-unstructured: the capability to conduct basic hacks against individual systems using tools created by someone else. The organization has little target analysis, command and control, or learning capability.

2. Advanced-structured: the capability to conduct more sophisticated attacks against multiple systems or networks and possibly to modify or create basic hacking tools. The organization possesses an elementary target analysis, command and control, and learning capability.

3. Complex-coordinated: the capability for coordinated attacks capable of causing mass disruption against integrated, heterogeneous defenses (including cryptography). Ability to create sophisticated hacking tools. Highly capable target analysis, command and control, and organizational learning capability.

Denning reported that the barrier for entry beyond the first level was quite high, and it would take any organization 2-4 years to progress from level 1 to 2, and another 6-10 years to advance to level 3. Terrorists have shown evidence mostly of level-1 activity but arguably progressing to level 2.

**Paying for Proxies.**

Terrorists might find it easier to pay third parties to carry out attacks for them, instead of developing their own skills. There are three reasons to believe this could be an appealing approach:

- A number of cybercrime organizations have been well established for several years. For instance, the Russian Business Network (RBN) is well known for creating the MPack malware kit and operating the Storm botnet. The cybercrime underground deals in malware, exploits, and attack tools, among other activities.
- A cyberarms race has been stimulated by Stuxnet. Virtually every modern country has been building up offensive and defensive cybercapabilities, usually within defense or intelligence agencies. For instance, the Iranian government reportedly has built a fairly capable hacker group, and Iran is friendly to terrorist groups such as Hamas and Hezbollah. As nations

around the world develop "cyber weapons," it will become easier for terrorists over time to acquire attack tools from friendly nations.

- New for-hire hacker groups (or "cyber mercenaries") are emerging to profit from working for clients. For example, security firm Symantec reported on a for-hire group of 50-100 hackers called Hidden Lynx.[30] The group is suspected of penetrating more than 100 organizations around the world since 2009, including U.S. defense contractors, investment banks, and security companies. It is suspected of compromising security firm Bit9 in 2012, a company that sells an "application whitelisting" service to other companies. By stealing the cryptographic keys for the Bit9 service, the hacker group was able to compromise other companies depending on that service, including military contracting firms. A smaller for-hire group called Icefog was reported by Kasperky Labs.[31] This group of 6-10 hackers seems to specialize in surgical hit-and-run attacks on the supply chain, using custom-made attack tools.

## VULNERABILITIES IN U.S. CRITICAL INFRASTRUCTURES

It is well known that about 90 percent of U.S. critical infrastructure is privately owned, consisting of a wide variety of custom-built equipment, though the sector is moving toward more common, off-the-shelf systems. Cybersecurity tends to be a low priority for system administrators, and systems are difficult to patch. Consequently, many vulnerabilities continue to exist. Often, a mixture of private and public networks

is used. Although the risks of public networks are well-known, private networks can also be equally vulnerable to intrusions, though owners tend to believe they are safer because they are not connected to public networks.

The number of vulnerabilities appears to be increasing rapidly. A recent vulnerability report by NSS Labs stated that SCADA/industrial control systems (ICS) vulnerability disclosures increased from 72 in 2011 to 124 in 2012; the count represents a 600 percent. increase from 2010.[32] The 124 vulnerabilities affect the products of 49 vendors.

Another vulnerability is the complexity and high connectedness of systems, which increases the risk of cascade failures (seen in past incidents with the power grid). The government states:

> This vast and diverse aggregation of highly interconnected assets, systems, and networks may also present an attractive array of targets to domestic and international terrorists and magnify greatly the potential for cascading failure in the wake of catastrophic natural or manmade disasters.[33]

Electric systems, as an example, are not designed to withstand or recover quickly from damage inflicted simultaneously on multiple components. A well-planned, coordinated attack could take down portions of the electric power system for a long time.

Although vulnerabilities exist, intruders need expertise to be successful, and chances are that only a small number of people have the necessary expertise for a given control system, which is often proprietary or customized. Although not many attacks on critical infrastructures have been publicized, attacks have been known to happen. In August 2012, Saudi Ara-

bia's state oil company, Saudi Aramco, saw more than 30,000 systems infected by a malware attack. Critical functions like oil production were unaffected, but basic oil operations were taken down. Shortly after, Qatar's liquified natural gas company, RasGas, suffered a malware attack that had the same *modus operandi*.

Cyberattacks might become easier, given the recent invention of the SHODAN search engine by John Matherly. SHODAN is a search engine that finds specific types of computers (routers, servers, etc.) using a variety of filters on service banners. SHODAN crawls the Internet for publicly accessible devices, concentrating on SCADA systems. Cybersecurity researchers use SHODAN to search for vulnerable SCADA systems. A student, Eireann Leverett, has used SHODAN to demonstrate he could find 10,000 ICS connected to the public Internet. These included water and sewage plants, which were easy to compromise due to weak security.[34]

## WHY NOT A MAJOR CYBERATTACK

Having established motive, means, and opportunity for terrorists, the natural question is why a major cyberattack has not happened yet. It seems that al-Qaeda and other terrorist groups still prefer bombs and physical attacks, even after Stuxnet.[35] In the absence of an attack, a case could be argued that cyberterrorism is more of a hypothetical threat than a real one.[36] However, there is debate about whether an actual cyberattack by terrorists has happened.[37] No major attacks have occurred, according to the public record, some observers have speculated that attacks have happened but have been kept confidential so as not to disclose weaknesses in the national infrastructure.

In 2007, Denning postulated three indicators that could precede a successful cyberterrorism attack:[38]

1. Failed cyberattacks against critical infrastructures, such as ICS. Unlike the case with the professionally developed Stuxnet, Denning expected that the first cyberterrorist attack would likely be unsuccessful, considering that even terrorist kinetic attacks frequently fail.

2. Research and training labs, where terrorists simulate their cyberattacks against targets, test attack tools, and train people. Israel reportedly had centrifuges at its Dimona complex to test Stuxnet on.

3. Extensive discussions and planning relating to attacks against critical infrastructures, not just websites.

So far, none of these indicators has been observed, which would imply that terrorists are not trying hard to prepare for cyberattacks.

Conway has argued against the likelihood of cyberterrorism in the near future.[39] Her argument consists of these reasons:

- Violent jihadis' IT knowledge is not superior.
- Real-world attacks are difficult enough.
- Hiring hackers would compromise operational security.
- For a true terrorist event, spectacular moving images are crucial.
- Terrorists will not favor a cyberattack with the potential to be hidden, portrayed as an accident, or otherwise remaining unknown.

Perhaps the most straightforward explanation of the lack of observed cyberattacks is the cost-benefit argument put forth by Giacomello.[40] He compared the

costs of traditional physical terrorist attacks with cyberattacks of the "break things and kill people" type. Specifically, Giacomello estimated the costs of three cyberterrorism scenarios aimed at the power grid; a hydroelectric dam; and an air traffic control system. If the power grid was viewed as an unlikely target, fatalities will be indirect or accidental. For a hydroelectric dam, the cost is based on a historical incident of an insider sabotaging the controls at the dam. Somewhat arbitrarily, the estimate assumed two proficient hackers with supporting personnel, totaling up to $1.3 million. For an air traffic control system, a higher number of skilled hackers are needed to compromise the system, prevent the air controllers from detecting and responding to the intrusion, and defeat built-in safety mechanisms. Again, it is not explicitly stated, but a year of work seems to be assumed, since the total is based on a year's salary. The resulting estimated cost was up to $3 million.

For comparison, Giacomello pointed out that the World Trade Center bomb cost only $400 to build, yet, it injured 1,000 people and caused $550 million of physical damages. The March 2004 attacks in Madrid, exploding 10 simultaneous bombs on four commuter trains using mining explosives and cellphones, cost about $10,000 to carry out. The 9/11 Commission Report stated that the 9/11 attacks cost between $400,000 and $500,000 to plan and execute.[41]

An examination of these comparative costs makes it clear that bombs are a much cheaper approach than cyberattacks by orders of magnitude. Stuxnet, estimated to have cost millions of dollars, does not change the cost-benefit comparison. At the present time and in the near future, cyberattacks of the "break things and kill people" type require an enormous amount of

effort by highly skilled experts. In contrast, bombs can be made cheaply and deployed without skilled effort. In addition, physical attacks are appealing because of the higher certainty of success.

This argument points to two fallacies in popular thinking. First, there is sometimes a misconception about the cost of cyberattacks. For example, Weimann stated that cyberterrorism would be attractive because cyberattacks require only a PC and Internet connection. This is true for simple attacks, but terrorists would aim for more sophisticated attacks requiring a high level of skill. Second, there was concern that Stuxnet could fall into the hands of terrorists, who would then use it against the United States. Clearly, by now, Stuxnet would no longer be effective after the world had seen its set of exploits. Although terrorists could modify Stuxnet for their own purposes, it is a high-precision weapon designed for a specific target. Terrorists would need to replace at least its payload and exploits, which would require a high level of expertise and time and still have an uncertain chance of success.

However, the cost-benefit argument does not completely rule out the possibility of cyberattacks as a means to complement physical attacks. In that case, the cyberattacks could be much more modest, not necessarily of the "break things and kill people" type. For instance, a cyberattack that takes down a communication network or emergency system during a crisis caused by a physical attack could be very effective in amplifying the total impact.

In addition, it is quite possible that development costs for Stuxnet-like malware could decrease in the future (as is usually the case with software and hardware). If that happens, the cost-benefit argument

could predict a point in the future when cyberattacks become attractive for terrorists.

## CONCLUSIONS AND RECOMMENDATIONS

Previous sections have examined motive, means, and opportunity for cyberterrorism. Our findings can be summarized as:

- Terrorists are familiar with IT technologies and depend on the Internet for many common activities, similar to most people.
- Terrorists are interested in cyberattacks but not at a high level of sophistication yet.
- Terrorists have not built up a high level of cyber skills or capabilities (e.g., acquiring zero-day exploits) yet.
- Instead of developing their own capabilities, terrorists might seek help from friendly nations or for-hire hackers.
- Vulnerabilities existing in national infrastructures present opportunities for cyberattacks but require a high level of expertise to exploit.
- The absence of cyberterrorist attacks might be explained most simply by a cost-benefit argument that physical attacks are orders of magnitude less costly than cyberattacks.
- Stuxnet has not seemed to have changed significantly the motive, means, or opportunity. And, despite concerns by some, it has not changed the cost-benefit trade-off either.

The last point implies that even after Stuxnet, terrorists still face a considerable cost barrier to carrying out large-scale cyberattacks. Therefore, such cyberattacks are probably unlikely in the near future. How-

ever, Stuxnet does have long-term implications, because the world has started on a cyberarms race. In the long term, there is likely to be a proliferation of major "cyber weapons," which might fall into the hands of terrorists.

There seems little that can be done to change motive for terrorists. Some have proposed the idea of deterrence, but it is questionable whether deterrence is possible in cyberwarfare in the same way that nuclear deterrence worked through fear of mutually assured destruction (MAD). Deterrence is predicated on the possibility of discouraging terrorists from attack by presenting a strong likelihood of retaliation. Unfortunately, the cyberenvironment is completely different from the nuclear environment, in which nuclear weapons can be traced and counted. In order to be effective, cyberdeterrence must overcome a few practical obstacles.

The first and most obvious problem is attribution—the identification of the real source of a cyberattack. Attackers have the advantage of plausible deniability in cyberspace. Attribution is difficult because cyberattacks can be anonymized in many ways. In malware attacks, the creator is very difficult to discover from code disassembly. The second practical problem, even if attribution can be solved, is credible capacity for destructive retaliation. Probably no one doubts the offensive capability of the United States, but it has not been demonstrated yet.

Also, there seems little that 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. Cybersecurity knowledge is freely available, and the barrier is low for terrorists to acquire training in cybersecurity.

The only factor that is feasible to address, then, is opportunity. Specifically, policies should enhance protection of national infrastructures to reduce the risk exposure to cyberattacks. Fortunately, the U.S. Government has already placed top priority on vulnerabilities in critical infrastructures, and a new Cyber Intelligence Sharing and Protection Act (CISPA) is under consideration, which is intended to facilitate security information sharing and enhance protection of critical infrastructures. However, it is not certain whether the Act will be sufficiently comprehensive and enforceable. For instance, some of the measures are voluntary rather than mandatory. Without mandatory measures to improve critical infrastructure security, it will be important to implement appropriate economic incentives to encourage desired actions.

Also, the National Infrastructure Protection Plan (NIPP) provides a unifying framework that integrates a range of efforts designed to improve protection of critical infrastructures. NIPP aims to prevent, deter, neutralize, or mitigate the effects of a terrorist attack or natural disaster, and to strengthen national preparedness, response, and recovery in the event of an emergency. It takes a risk-management approach consisting of identifying assets and assessing threats and vulnerabilities.

All measures to reduce the opportunity for cyberterrorists are recommended. However, the adaptiveness and resourcefulness of terrorists should not be underestimated. The NIPP says:

> As security measures around more predictable targets increase, terrorists are likely to shift their focus to less protected targets. Enhancing countermeasures to address any one terrorist tactic or target may increase the likelihood that terrorists will shift to another.[42]

The openness of the security problem means that it will be practically impossible to fix every vulnerability and eliminate all opportunities for terrorists. Perhaps policies should recognize that cyberattacks are 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.

## ENDNOTES


1. C. Cratty, "FBI on Guard against Terrorist Cyber Attacks,"CNN, March 16, 2012, available from *edition.cnn.com/2012/03/15/us/cyber-attacks*.

2. G. Weimann, "Cyberterrorism: How Real is the Threat?" Washington, DC: United States Institute of Peace, December 2004, available from *www.usip.org*.

3. B. Collin, "The Future of Cyberterrorism," *Crime and Justice International Journal*, March 1997, p. 15.

4. Dorothy Denning, "Cyberterrorism—Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives," Washington, DC: U.S. House of Representatives, May 23, 2000, available from *www.stealth-iss.com/documents/pdf/CYBERTERRORISM.pdf*.

5. Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: the Internet as a Tool for Influencing Foreign Policy," J. Arquilla and D. Ronfeldt, eds., *Networks and Netwars*, Santa Monica, CA: Rand, 2001.

6. "Patterns of Global Terrorism 2003," Washington, DC: U.S. Department of State, April 2004, available from *www.state.gov/documents/organization/31912.pdf*.

7. C. Wilson, "Computer Attack and Cyberterrorism: Vulnerabilities and Policy Issues for Congress," Congressional Research Service (CRS) Report for Congress RL32114, Washington, DC: CRS, April 2005.

8. "Stuxnet under the Microscope 1.3," Eset, 2010, available from *go.eset.com/us/resources/white-papers/Stuxnet_Under_the_Microscope.pdf.*

9. "W32.Stuxnet Dossier Version 1.3," Symantec, November 2010, available from *www.symantec.com/content/en/us/enterprise/media/security_response/ whitepapers/w32_stuxnet_dossier.pdf*.

10. F. Petruzella, *Programmable Logic Controllers*, Boston, MA: McGraw Hill Higher Education, 2005.

11. H. Berger, *Automating with SIMATIC*, Erlangen, Germany: Publicis Corporate Publishing, 2003.

12. D. Sanger, "Obama Order Sped up Wave of Cyberattacks against Iran," *The New York Times*, June 1, 2012, available from *www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html*.

13. P. Brunst, "Terrorism and the Internet: New Threats Posed by Cyberterrorism and Terrorist Use of the Internet," M. Wadea and A. Maljevic, eds., *A War on Terror: The European Stance on a New Threat, Changing Laws and Human Rights Implications*, New York: Springer, 2010.

14. G. Giacomello, "Bangs for the Buck: A Cost Benefit Analysis of Cyberterrorism," *Studies in Conflict and Terrorism*, Vol. 27, 2004, pp. 387-408.

15. Brunst.

16. Office on Drugs and Crime, "The Use of the Internet for Terrorist Purposes," New York: United Nations, September 2013, available from *www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf*.

17. Dorothy Denning, "Terror's Web: How the Internet is Transforming Terrorism," Y. Jewkes and M. Yar, eds., *Handbook on Internet Crime*, Abingdon, Oxon, United Kingdom (UK): Willan Publishing, 2009.

18. Stephen Ulph, "Internet Mujahideen Refine Electronic Warfare Tactics," Washington, DC: The Jamestown Foundation, February 7, 2006, available from *www.mafhoum.com/press9/268T44.htm*.

19. *Ibid*.

20. *Ibid*.

21. A. Hall, "Al-Qaeda Chiefs Reveal World Domination Design," *The Age*, August 24, 2005, available from *www.theage.com.au/news/war-on-terror/alqaeda-chiefs-reveal-world-domination-design/2005/08/23/1124562861654.html*.

22. "Al-Qaeda Cyber Capability," Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis TAV01-001, Ottawa, Ontario, Canada: Government of Canada, November 2, 2001.

23. P. Brush, "Use of Web in Terror Attack Feared," CBS News, February 11, 2009, available from *www.cbsnews.com/stories/2002/06/27/attack/main513582.shtml*.

24. B. Gellman, "Cyber-attacks by Al Qaeda Feared," *The Washington Post*, June 27, 2002, available from *www.washingtonpost.com/wp-dyn/content/article/2006/06/12/AR2006061200711.html*.

25. W. Matthews, "Al Qaeda Cyber Alarm Sounded," July 25, 2002, available from *fcw.com/articles/2002/07/25/al-qaeda-cyber-alarm-sounded.aspx*.

26. S. Ackerman, "Pentagon Deputy: What if al-Qaeda Got Stuxnet?" February 15, 2011, available from *www.wired.com/2011/02/pentagon-deputy-what-if-al-qaeda-got-stuxnet/*.

27. R. Mueller, "Speeches—RSA Cyber Security Conference, San Francisco, CA, March 04, 2010," available from *www.fbi.gov/news/speeches/tackling-the-cyber-threat*.

28. Giacomello, pp. 387-408.

29. Denning, "Cyberterrorism."

30. D. Goodin, "Meet Hidden Lynx: The Most Elite Hacker Crew You're Never Heard Of," September 17, 2013, available from *arstechnica.com/security/2013/09/meet-hidden-lynx-the-most-elite-hacker-crew-youve-never-heard-of/*.

31. Kaspersky Lab, "The Icefog APT: A Tale of Cloak and Three Daggers," September 25, 2013, available from *www.securelist.com/en/blog/208214064/The_Icefog_APT_A_Tale_of_Cloak_and_Three_Daggers*.

32. S. Frei, "Vulnerability Threat Trends," 2013, available from *www.nsslabs.com/reports/vulnerability-threat-trends*.

33. "National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency," Washington, DC: U.S. Department of Homeland Security, 2009, available from *www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf*.

34. K. Zetter, "10k Reasons to Worry about Critical Infrastructure," January 24, 2012, available from *www.wired.com/threatlevel/2012/01/10000-control-systems-online/*.

35. Dorothy Denning, "Stuxnet: What Has Changed," *Future Internet*, Vol. 4, 2012, pp. 672-687.

36. Weimann.

37. Brunst.

38. Dorothy Denning, "A View of Cyberterrorism Five Years Later," K. Himma, ed., *Readings in Internet Security: Hacking, Counterhacking, and Society*, Boston, MA: Jones and Bartlett, 2007.

39. M. Conway, "Against Cyberterrorism," *Communications of ACM*, Vol. 54, No. 2, February 2011, pp. 26-28.

40. Giacomello, pp. 387-408.

41. "The 9/11 Commission Report," Washington, DC: National Commission on Terrorist Attacks Upon the United States, available from *govinfo.library.unt.edu/911/report/index.htm*.

42. "National Infrastructure Protection Plan."

**U.S. ARMY WAR COLLEGE**

**Major General Anthony A. Cucolo III**
**Commandant**

*****

**STRATEGIC STUDIES INSTITUTE**
**and**
**U.S. ARMY WAR COLLEGE PRESS**

**Director**
**Professor Douglas C. Lovelace, Jr.**

**Director of Research**
**Dr. Steven K. Metz**

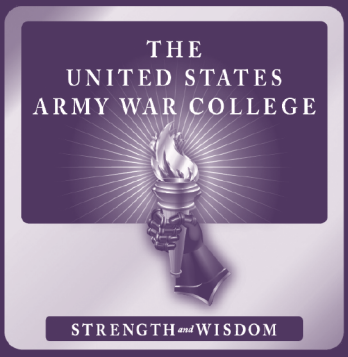
**Author**
**Dr. Thomas M. Chen**

**Editor for Production**
**Dr. James G. Pierce**

**Publications Assistant**
**Ms. Rita A. Rummel**

*****

**Composition**
**Mrs. Jennifer E. Nevil**


FOR THIS AND OTHER PUBLICATIONS, VISIT US AT
http://www.carlisle.army.mil/

ISBN 1-58487-627-1


This Publication

SSI Website

USAWC Website