Information Warfare and Strategic Terrorism

FRANK J. CILLUFFO AND CURT H. GERGELY

In their article, Matthew Devost, Brian Houghton and Neal Pollard explore the potential impact of information terrorism on US national security and the welfare of American citizens. While we agree with a number of the points in this article, we believe that it overlooks the potential implications for terrorist use of information warfare (IW) techniques in a strategic context. We believe that the threat posed by terrorist use of IW techniques exceeds that described in the article. A dedicated adversary can procure and employ capabilities that present a grave threat to US national security, specifically: a synergistic attack that capitalizes on IW strategies to multiply the effects of traditional terrorist tactics.

The examples of information terrorism provided by Devost, Houghton and Pollard are relatively limited in scope, and it is questionable whether they would have caused the reactions that the authors have stated. While the American public may be casualty adverse, it is unlikely that the public would insist that the President abrogate an agreement with our NATO partners because two aircraft were lost and the computers of curious bystanders damaged through the introduction of malicious code. Furthermore, IW extends the traditional battlefield to include societal centers of gravity, offering many more attractive targets which would maximize disruption, create collateral damage (physical and psychological) and compound lethality. Many of these targets can be attacked remotely, and terrorists often select 'soft targets'. In an increasingly interconnected world the United States can no longer rely on the physical isolation provided by the Atlantic and Pacific Oceans, or forward deployed military forces to prevent an attack within the Continental United States. The United States has lost its defensive sanctuary, and critical components of our information networks and infrastructure systems are open to attack by a well-informed adversary.

Information warfare includes actions taken to achieve information superiority by affecting adversary information and information systems

Terrorism and Political Violence, Vol.9, No.1 (Spring 1997), pp.84–94
PUBLISHED BY FRANK CASS, LONDON

while leveraging and protecting one's own information and information systems. Offensive IW may be carried out through physical attacks, the use of special technologies,[1] computer intrusion and computer warfare, electronic warfare, psychological operations and the use of strategic and military deception supported by intelligence collection and analysis. A number of nations have adopted similar doctrinal concepts including the United States, Russia, the People's Republic of China and France. A unique attribute of IW is that it can be pursued throughout the spectrum of conflict. Terrorist groups also have the ability to conduct limited scale IW attacks. Although there has been no evidence to date that they intend to conduct such activities, these groups could launch effective attacks with access to appropriate targeting data. Unfortunately, much of the data required to successfully target and attack critical information system functions and critical infrastructure facilities is available through open source analysis.

In the following sections we will examine the changing nature of terrorism, discuss the attributes of IW and the potential impact and consequences of an IW attack, examine the vulnerability of the United States to an IW attack, and describe the risks of such attacks. In the final portion of the article, we will present recommendations for dealing with the use of IW tactics by terrorists.

The Changing Nature of Terrorism

Most definitions of terrorism are limited and generally do not consider the entire range of motives and actions that may be used by a terrorist organization to intimidate, coerce or influence a targeted population. Terrorism is generally defined as the premeditated, politically motivated use of violence perpetrated against noncombatant targets by subnational groups or clandestine state agents. It has been traditionally seen as armed propaganda or propaganda of the deed. According to this view, the purpose of a terrorist attack is to influence a target audience to acquiesce to the political views of the terrorist group. Terrorist groups are seen as having political objectives which constrain their use of extreme measures for fear of losing the allegiance of the public.

This traditional view of terrorist motivation is most familiarly applied to leftist political groups, such as the Red Army Faction, the Red Brigades, Direct Action or the foci movements in Latin America. However, it may be a poor construct for analyzing the motivations of the terrorist groups that currently present the greatest threat to the security of the United States and its allies. These groups are generally motivated by religious fanaticism, racial or ethnic hatred, or severe alienation from the United States and its government. Such groups are not constrained by a political ideology, nor do they strive for popular support and acceptance. They are motivated by the desire for revenge, retribution or punishment. As a result, attacks are designed to cause the greatest potential damage to high visibility or symbolic targets.

In general, terrorists achieve their objectives through the use of violence. The most jarring examples of terrorism are those that cause large numbers of deaths or great destruction. In recent years the number of terrorist incidents has actually declined; however, terrorist incidents have increased in lethality. Terrorist incidents have become more deadly and have moved into the age of mass casualty attacks with the use of the nerve agent Sarin in the Tokyo subway system. This trend is unlikely to be replaced by a kinder, gentler information-based terrorism. Terrorist organizations are more likely to seek the capability to conduct super-terrorist incidents with massive casualties which will truly terrorize the targeted nation, and will cause a strategic accommodation with the terrorist organization. This terrorist capability could well be achieved though the planned, synergistic use of very large conventional explosives, weapons of mass destruction (WMD), IW and infrastructure warfare techniques.

The effects of a well-planned terrorist attack using these elements could be devastating and is within the realm of possibility. Modern terrorist organizations are increasingly technology literate and are making use of high technology to execute their objectives. Terrorist groups are using advanced technologies to obtain information, plan attacks and conduct attacks. While it is unlikely that a terrorist group could execute an attack that would affect the entire nation, they could conduct attacks that would affect major cities or regions of the United States. Such attacks would likely feature applications of IW, which would augment the destructiveness of traditional terrorist tactics.

Terrorist Use of Information Warfare

Information warfare provides a significant capability that could be used by terrorists to attack US national interests directly and indirectly. As we noted before, information warfare is more than computer intrusion and computer-based attacks. It also includes physical destruction, electronic warfare, deception, psychological operations and operations security measures. Terrorist organizations have demonstrated some capability in each of these areas. What differentiates IW from other activities is that these capabilities are focused on information systems and the information that they contain. Terrorist groups using an IW paradigm to guide their actions would seek to determine their adversary's critical information nodes and target them for destruction or exploitation. These groups would also seek to protect their own information systems to prevent them from being attacked or exploited. However, due to the heavy dependence of the US on networked information systems, terrorist groups will enjoy a disparate advantage in the offensive applications of IW.

Terrorists may seek an IW capability as a means to attack critical information systems operating in the United States and other nations. Terrorists have undoubtedly noticed that the dependence of the United States and other industrialized nations on information and communications systems is growing at near exponential rates. Virtually every facet of an industrial nation's existence depends upon a functioning telecommunications system and the interconnected, networked information systems supporting vital functions such as banking and finance, health services, electric and power distribution, transportation, defense and the operation of the various infrastructure systems. In general, these information systems have been engineered in the most economically effective manner. As a result, they often lack redundancy and may be dependent on a relatively small number of critical nodes. Carefully planned attacks on relatively few nodes may cause large, prolonged outages disrupting extremely large populations. As a result, the terrorist group may be able to achieve a disproportionately large impact from a limited number of operational activities.

A terrorist group could achieve a rudimentary information attack capability fairly quickly. Critical facilities such as switching centers or Internet router hubs could be attacked using conventional explosives, stand-off munitions or incendiaries. Persistent chemicals, biological agents or radioactive isotopes could be combined with an explosive device or spread surreptitiously in a key facility to prevent its use. Terrorists could develop computer intrusion and computer attack capabilities within their groups or recruit hackers (sometimes unwittingly) with similar views to attack computerized networks. Terrorists could also obtain electronic warfare jammers to attack radio systems, communications satellites and microwave transmissions.

Information Systems in Support of Terrorist Activities

Along with attack capabilities, terrorist organizations are also exploiting information technologies as a tool in support of their operations and campaigns to collect intelligence, to communicate and for propaganda purposes. Given today's state of technology, and the inherent dual-use applications, terrorist groups can procure a cheap yet robust communications intelligence (COMINT) collection capability, unattainable and unimaginable just a couple of years ago. Through computer intrusion techniques such as hacking into the public switched telecommunications network (PSTN) or other COMINT methods, terrorists can intercept valuable political, economic or military secrets. They can also be expected to run countersurveillance on law enforcement (to thwart operations, identify informants, etc.) and even perform profiling analyses in order to identify individuals who can be bribed, co-opted, coerced or 'neutralized'. Taking advantage of powerful search engines on the Internet in conjunction with sophisticated software available on underground hacker bulletin boards, terrorists can map and analyze critical nodes that can be exploited for intelligence collection purposes or for target acquisition and selection for future attacks. Furthermore, most of the intelligence collection can be done anonymously, by concealing one's identity or even 'masquerading' as someone else. Terrorist groups can also utilize publicly available software to process and analyze the raw information in order to create a complete intelligence product.

Aside from intelligence collection, terrorist organizations are maximizing advanced technology for communications and tradecraft purposes. The Internet and other information systems provide terrorist groups a global and near real-time command and control communications capability. Single-level cell structures can be established between a 'handler' or military planner and his operatives. Compromising one element would not jeopardize the entire terrorist network, as the operatives would be compartmented. The availability of sophisticated encryption devices and anonymous remailers also enable relatively secure communications or stored data, greatly impeding law enforcement's monitoring abilities – and even those of the Intelligence Community – when the source is of foreign origin. Even if terrorist communications are successfully compromised, an adept terrorist organization can circumvent law enforcement or intelligence countermeasures by using pre-determined codewords initiating a phase of the operation or activating long-term 'sleepers'.

Modern media applications offer terrorists a low cost yet powerful means to spread their propaganda – often disinformation – to millions of people worldwide. A number of terrorist groups such as the Sendero Luminoso, the Revolutionary Armed Forces of Columbia (FARC), the Liberation Tigers of Tamil Eelam (LTTE) and racial identity groups have established web sites on the Internet which include their ideologies, manifestos and communiques. These virtual public relations headquarters and safehavens in cyberspace are intended to gain popular political and financial support. It is presently estimated that more than 40 million users are connected to the Internet. Aside from the potential implications and damage caused by the individual sites themselves, the proliferation of such propaganda sites and affinity groups legitimize and reaffirm aberrant attitudes globally, perhaps even forging alliances of convenience. They also serve as avenues to share and disseminate information.

The advent of CNN and other global 24 hour news stations provide adversaries a vehicle to conduct sophisticated psychological operations in real-time.[2] It is only a matter of time until terrorists realize how they can leverage and capitalize on this method in order to influence the US population and hence policy. The US government has not adequately investigated how to best respond to this phenomenon.

Vulnerability of the United States

The United States is extremely vulnerable to a well planned terrorist attack that uses IW as a component. Numerous articles have noted the vulnerability of the telecommunications system, the control systems of networked infrastructures, electronic fund transfer systems and defense communication systems to information attacks.[3] Due to the growing interconnection of these networks, it is likely that an attack on one information network will affect all interconnected networks. An example of this problem is the public switched telecommunications network (PSTN).

The PSTN has experienced a significant number of hacker attacks and, as a result, its vulnerabilities are well documented in hacker publications, hacker bulletin board systems and on various World Wide Web sites. Additionally, the tools needed to conduct a computer-based attack are available through many of the same hacker bulletin boards and web sites. The physical addresses of the various telecommunications facilities are available through sources as diverse as *2600 Magazine* and the Local Exchange Routing Guide published by Bellcore which also lists the attributes of these facilities. Additional information which would provide insights for targeting is available from the Federal Communications Commission, state Public Utility Commissions, trade journals and the various telecommunications carriers.

While it is extremely unlikely that a terrorist group could adversely affect telecommunications across the United States, depriving a region or major metropolitan area of telecommunications support for a protracted period is a distinct possibility. The impact of such an attack could be significant. The implications would depend on whether the telecommunication system was attacked in isolation, or whether other facilities were simultaneously attacked. Even an isolated attack on the telecommunications system would destroy all telecommunications services including those required for police, fire and emergency medical services in a regional area. The potential for public disorder and deaths resulting from fires and medical emergencies would increase significantly during the period that the telephone system was inoperable. If the area attacked also contained an Air Route Traffic Control Center (ARTCC), it is likely that all air traffic would have to be suspended in the area under the stricken ARTCC's control. The National Transportation Safety Board noted in March 1996 that 16 of the 21 ARTCCs were totally dependent on the PSTN for communications and data links. Aircraft in the area would have to be controlled using manual procedures. The length of the outage would depend on the portion of the PSTN attacked, and the ability to repair the portion damaged. A key consideration for telecommunications systems is that switches are generally designed for the specific facility in which they are used. As a result, they are often not readily interchangeable and would be difficult to replace in a timely fashion.

If the attack above were combined with an IW attack on the electric power system or with an infrastructure warfare attack on the electric system, the situation would be significantly worse. Depending upon the portion of the electric power system attacked, a power outage could last anywhere from hours to months. A major city without lights or telephones would rapidly become chaotic, requiring the mobilization of the National Guard and the implementation of curfews, rationing and other emergency measures. Virtually all services in the city attacked would come to a halt, affecting businesses, individuals and government. A sustained outage in a major metropolitan area could result in losses of millions of dollars per day in lost sales and wages. Recovery would be protracted due to the dependence of the electric power and telecommunications systems on each other. Virtually all other networked infrastructure systems would also be adversely affected. There would be a significant potential for cascading failures in the impacted region.

In an extreme example, a terrorist could conduct an attack using a biological or chemical agent, and then use information warfare and infrastructure warfare techniques to attack key information systems and infrastructures to hamper recovery and reconstitution efforts. The effects from such an attack would be widely felt, shocking the entire world community. This final type of attack would most closely fall into a concept of strategic terrorism, the worst manifestation of which would be a decapitating attack on Washington, DC or another national capital. Although the potential for such an attack may be low, it cannot be completely discounted. Information warfare could play a decisive role in such an event by preventing communications from going in or out of the stricken area or by providing erroneous information to responding emergency units. It could also be used to attack information systems in responding medical activities, or to attack key information systems required to support other response activities.

All of these attacks would be witnessed by a world community which would reasonably be concerned about its safety. The terrorist group could then reinforce its position through skillful use of psychological operations and deception.

Conclusions

Terrorist use of IW presents a significant threat to US national security interests; however, this threat is most significant when IW is part of a combined terrorist campaign. The potential for an electronic Pearl Harbor based solely on information attacks, especially when based strictly on computer-based attacks, is likely overrated, and the chances of it happening could be greatly reduced through the prudent use of information security countermeasures. A far more serious threat is posed by the synergistic use of all the attributes of IW with the use of other traditional and non-traditional terrorist activities.

Recommendations

The United States must be prepared to defend and effectively respond to information warfare and strategic terrorism. Given the dynamic and ubiquitous nature of the threat, close coordination and information sharing between and among the Intelligence Community, law enforcement, the private sector, and agencies and entities responsible for emergency preparedness and consequence management is critical. Similar to conventional terrorism, US response options must remain flexible and be determined on a case by case basis. What works most effectively in one case may not incur the same leverage or desired outcome in another. Response options can range from law enforcement measures, to diplomacy and economic sanctions, to covert action and clandestine means, to full-scale military intervention and reprisal.

While we agree with some of the recommendations made by Devost, Houghton and Pollard, we do not agree with many others, and would suggest a notably different set of options for the nation's policy makers. First, we believe that the cornerstone of the nation's information assurance policy must be based on adequate use of protective measures. While there are no protective measures that are completely effective, in many cases the '80 per cent' solution will be sufficient to deter attackers by increasing the risk of detection or failure. Protective measures should be based on an acknowledged national information assurance strategy. Second, we must reallocate and manage our intelligence assets in such a way as to assure that decision makers and security planners develop an accurate, comprehensive understanding of the threat posed by terrorist use of IW or other high technology attack capabilities. Third, we need to develop and institutionalize within the parameters of Presidential Decision Directive 39, crisis and consequence management procedures for an IW attack. Fourth, we need to develop retaliatory options that respond to the threat posed by information attackers in a rational manner. This plan would provide the President with a range of options commensurate to the scope of the attackers. Fifth, we need to drastically improve our indications and warning capability for IW attacks, which is currently minuscule. This function should be shared between the Federal Bureau of Investigation and the National Security Agency/Central Security Service.

We do not agree with the recommendations to establish a *Special Security Directorate* at the National Security Council (NSC). The NSC was not staffed or created to be an operational entity. The number of issues that the proposed 'Czar' would be responsible for are so broad that he would be immobilized by politics and bureaucratic inertia. In this case, the Office of National Drug Control Policy, which has been largely ineffective, is a very apt comparison. We also do not endorse the creation of a freestanding system of *Digital Integrated Response Teams*, as the majority of the retaliatory functions assigned to this team as outlined would be a violation of US Code and in some cases would constitute an act of war.

Currently, the ability of the United States to deter and mitigate such attacks is fragmented at best. We propose that the following actions be taken to enhance US capabilities for risk mitigation. The IW threat posed by terrorists must be addressed in the context of an Information Assurance strategy. Portions of this strategy include:

- *Develop a Presidential Decision Directive and an Executive Order defining and implementing a National Information Assurance Policy.* This policy should establish an Information Assurance Board within the Executive Branch, define the roles of the federal agencies for information assurance and specify the intelligence and domestic law enforcement functions required to counteract information attacks that may involve US citizens and foreign powers. This guidance must strike a balance between civil liberties and national security.
- *Mandate High Priority Intelligence Collection Requirements concerning terrorist use of IW.* The Intelligence Community must coordinate and increase all source intelligence collection requirements for terrorist use of IW. The Intelligence Community must re-examine collection methods for information acquisition (unique Signals intelligence) and cultivate sources (both in terms of recruiting agents in cyberspace and more traditional HUMINT methods) in order to gain a clear understanding of

the threat in terms of actors, motives, capabilities and *modus operandi*. Close cooperation between the collectors and analysts within the Intelligence Community is crucial. The National Intelligence Council should sponsor a National Intelligence Estimate to establish a baseline for threat analysis within the Intelligence Community and to sensitize national leaders to the potential threat.

- *Establish an Information Warfare Indications and Warning Center.* The United States needs the ability to provide decision makers with detailed analysis of indications of an information attack. This capability could be distributed through several analytical centers which would coordinate the development of warnings. This capability should be under the direction of the National Intelligence Officer for Warning to support this individual's ability to provide the President with strategic and operational warning of attacks that may detrimentally affect the capabilities of the United States.
- *Establish Crisis Management and Consequence Management Responsibilities for Information Warfare Attack.* In line with the specific guidance provided for counterterrorism efforts, the President should establish crisis and consequence management responsibilities for information attacks. They should include defining roles and missions, planning reconstitution and continuity of government and operations.
- *Establish a set of Pre-examined National Strategies and Response Options.* The National Security Council and the Joint Chiefs of Staff should establish a set of retaliatory options for information attacks similar to the limited nuclear options contained in the Single Integrated Operations Plan (SIOP) for use by the President in the case of an offensive IW campaign against the United States. The US should publicly announce it will vigorously pursue all attackers using the entire range of military options or law enforcement activities in order to deter an incident before it occurs.

NOTES

[1] Special technologies include non-lethal biological and chemical effectors, liquid metal embrittlement, carbon fiber, directed energy and other applications of technology designed for the express purpose of disrupting or disabling an adversary's support and operational capabilities.

[2] This was best exemplified by Somali warlord Mohammed Farrah Aideed's use of television to convince the US leaders that the US could win militarily in Somalia, but only at a cost that was politically untenable. The most significant aspect of this campaign was the ambush of US Army Rangers attempting to apprehend members of Aideed's militia, and the subsequent scenes of soldiers' bodies being dragged through the streets of Mogadishu which were broadcast live on CNN and successively replayed on the nightly news. Aideed realized the susceptibility of the American people to such a campaign due to the failure of US leaders to

adequately explain our national interests in Somalia, and an unwillingness to admit the potential for casualties. We believe that these effects could have been mitigated with a clear statement of national security objectives.

3. It should be noted that an attack by an intelligent adversary would have far greater consequences than would result from a natural disaster. This is due to the relatively low number of critical assets and the engineered resilience of infrastructure systems. Due to the low number of critical facilities the probability for the destruction of a particular facility as the result of an untargeted event is very low. Only in the case of targeted attack does the destruction of a critical infrastructure facility or information network become a high probability event.