# ARTICLES

## AN INTRODUCTION TO THE IMPACT OF INFORMATION TECHNOLOGY ON NATIONAL SECURITY

THE HONORABLE PORTER GOSS*

### EDITORIAL NOTE

On April 20-21, 1998, Duke University hosted a two-day conference entitled "National Information Infrastructure Protection in the 21st Century". The keynote address, presented by Representative Porter Goss (R-Fla.) is reproduced here. While the address has been reproduced as closely as possible to the original form in which it was presented, some formatting and grammatical changes were necessary to assist the reader and provide clarity.

### I. INTRODUCTION

The following discussion addresses current issues surrounding information technology and national security, first by examining the newfound complexity of threats facing the United States in a post cold-war world, and then by reviewing the development of effective strategies to protect domestic information infrastructure from outside attack. While there are many obstacles to an effective defense strategy, the United States must both confront threats posed by a potential misuse of information technology and harness that technology as a tool to benefit modern life.

---

* Congressman Goss, Member, United States House of Representatives, is the current Chairman of the House Intelligence Committee and was selected for the role after serving only one term on the Committee. He has also served on the House Foreign Affairs Committee, the House Rules Committee, and the House Ethics Committee. In addition, he has been active on the Bipartisan Ethics Reform Task Force and served as a Deputy Republican Whip in the House of Representatives. Before his career in politics, Congressman Goss spent two years in Army Intelligence and a decade as an intelligence officer in the Central Intelligence Agency. The views expressed in this Article are those of the author alone and are not to be construed as the position of the House Permanent Select Committee on Intelligence.

## II. THE EVOLUTION OF U.S. NATIONAL SECURITY

A strident national defense policy requires preparation, proactivism, and wisdom, all of which should be incorporated into a strategy that addresses the changing face of challenges to U.S. national security. As the nature of these challenges changes, different weak links develop. Pearl Harbor, Khobar Towers, and the World Trade Center serve as reminders of American vulnerabilities. However, today's vulnerabilities differ from those of just a few years ago, and call for new tactics.

Until recently, national security was a simple strategy designed to respond to three overt movements: aggression, expansionism, and territorial imperative. Earlier in this century, U.S. defense strategy tackled Prussian militarism and, in the Second World War, Nazism and Japanese totalitarianism. As aggressive expansionism led communism to spread around the globe, President Ronald Reagan advocated action in response to the red ink radiating across the world map. The United States confronted the communist-generated "hot" wars in Korea and Vietnam and the quiet war in Afghanistan. The red ink representing Communism provided a tangible threat, shaping a distinct U.S. national security policy.

The period of communist expansionism brought with it the threat of nuclear war. The Johnson Administration's ad campaign left a vivid impression: a little girl in a field of flowers with a mushroom cloud in the background. That image profoundly expressed the real concerns about the gut-wrenching problem of nuclear war. President Clinton repeatedly assuages the American people of this threat, stating that today's children can sleep without worry because there are no longer nuclear warheads pointed at them. Children would not sleep so soundly if they knew how little time it would take to re-aim those rockets and prepare them for launching. The threat of nuclear war remains, and the end of the Cold War does not signal the end of a need for strong national security.

### A. The Public and National Defense

The United States needs to build a constituency who understands the importance of a strident defense strategy. Today, due to a high standard of living and the nature of modern threats to U.S. national defense, American citizens suffer from apathy about national security. For example, recent American military engagements in countries such as Haiti, Nicaragua, and Panama seem safely removed from American shores. The American people have difficulty imag-

ining the navies of those countries setting sail and threatening U.S. harbors or borders, making it increasingly difficult for people to recognize modern problems of national security. Even more disturbing than apathy, some Americans have expressed a distrust of government. Joseph Nye of Harvard's Kennedy School of Government has discussed this phenomenon. These citizens do not see the role of government as protective and defensive, but rather as threatening or dangerous. The recent incidents in Waco, Ruby Ridge, Texas, and Oklahoma City demonstrate that modern American society houses extremely diverse viewpoints on both the current status and the ideal role of government in the United States. Whether these phenomena represent calculated disinterest or apathy, they stem from the failure of leaders to supply a consistent national defense policy with which the American people can identify.

### B. The Ad Hoc Nature of American Foreign Policy

Today, the U.S. government attempts to allay any public fear of threats facing national security, while conducting foreign policy on an ad hoc basis. The United States has a need for a consistent strategy, so that the American people can develop a stronger national identity and better comprehend the changing challenges to it. There remain many external threats to U.S. national security for which a consistent national defense strategy should be devised. Some examples are the current situations in Russia, China, Iraq, and Cuba.

Current economic conditions in Russia have caused quality of life to deteriorate for the Russian people and have created a widespread sense of poverty—even within the former military elite. This has placed pressures on the chain of command of the Strategic Rocket Forces. Furthermore, the economic situation has also created a burgeoning market for all kinds of things useful for mischief, such as suitcase nukes. Some of the Russian people with whom we are cooperating on a confidential basis in response to the anti-proliferation issue seem to be less than honorable in their dealings with us. In fact, there is evidence that our partners in negotiation are complicit in the sale of technology to our enemies. This is not a comfortable situation, even if the rockets are not pointed at us.

While President Clinton claims that China has "changed its cheating ways" when it comes to proliferation technologies, it is impossible to overlook China's long, sordid history as a proliferator. Perhaps China has improved its ability to deceive the United States, or perhaps the United States suffers from a dulled perception of the

threat posed by China. In either case, the United States must carefully track its exports of advanced technologies to China. For example, the United States must carefully weigh the costs and benefits of domestic businesses entering Chinese nuclear reactor market, an aggressive, competitive field reportedly worth $50 billion. While U.S. businesses and trade should not be disadvantaged in any way, it is necessary to remain wary of China's track record. The United States should not give the Chinese materials that could later provide us with an unwanted surprise.

Iraq serves as another example of an external threat to U.S. national security. Saddam Hussein appears to have no compunction in using misinformation as a psychological weapon, and he uses it to amplify or create substantial collateral damage, even where there is none. Such information warfare is not fair play, and it would be unwise for the United States to mimic these tactics in a quest to destabilize Hussein. If the United States were to carpet bomb Iraq in its efforts to sanction Hussein, there would be many innocent victims, both real and invented by Hussein. Instead, the United States should apply the lessons gleaned from its relationship with Cuba. After a long history with Cuba, the United States has learned that the origin of the problems is not the Cubans but Fidel Castro. Likewise, the origin of the Iraq problem is not the Iraqis but Saddam Hussein. To minimize the costs to innocent victims, the United States should develop a foreign policy that focuses on Saddam Hussein, and avoids injuring the innocent people of Iraq.

In addition to the troubling areas mentioned above, there are a number of other transnational threats to American national security. The United States must update its defense strategy in response to threats such as terrorism, narcotics, trafficking, and racketeering—threats that pay little regard to national boundaries. Unfortunately, U.S. congressional oversight is tailored to traditional threats and thus to threats contained within the confines of national sovereignties. As the scope of terrorist activity spans beyond these boundaries, Congress' traditional tools fail to address the problem efficiently.

The United States lacks—and desperately needs to develop—a coherent strategy for ensuring national security in this new era. Unfortunately, today's American foreign policy consists of nothing more than a series of disjointed and ad hoc reactions to external international situations. Although the United States no longer faces the overt threats of the past, dangers remain, and continue to change

rapidly. The United States must define a new model in response to threats generated by changing technology.

## III. ADDRESSING THREATS TO INFORMATION INFRASTRUCTURE: THE AMERICAN MODEL

The United States is combating the threat to its technology infrastructure with a policy model designed for traditional foreign policy and national security systems, and now is in danger of suffering an "electronic Pearl Harbor." Because computers are now such an integral part of American life, the nation is particularly vulnerable to electronic attack. American dependency on computers creates vulnerabilities ranging from the everyday, such as bank accounting or Floridian air conditioning, to the life-threatening, such as air traffic control. The potential targets are endless. As with its approach to traditional national security, the U.S. government's approach to this new threat is reactive and ad hoc. Frankly, we are not prepared.

Recent experience has proven that even the most crucial American military computer systems are not secure. In 1997, the Department of Defense (DOD) responded with *Eligible Receiver*, an interesting and highly commendable exercise that focused on the vulnerability of U.S. information infrastructure. The simulation team's operations were restricted by many rules, the most important of which was that no U.S. laws could be broken. The team was not allowed to use any secret or classified tools, thus limiting its techniques to those derived solely from open source research. No "insider" information was provided and no "collateral" intelligence was allowed. Every element of the attack had to exploit an actual, real-life vulnerability of the target system. Although the members of the *Eligible Receiver* team operated with their hands tied behind their backs and were given only three months to complete the exercise, their findings were dire.

There are many discrepancies between *Eligible Receiver* and reality. For example, if *Eligible Receiver* had been performed by a real attacker, in order to minimize detection, the hacker would have gone after systems that were poorly protected, finding much information. Moreover, the "attacks" represented by *Eligible Receiver* could result only in the denial of service, which pales in comparison to the dangers posed by threats such as intelligence collection and data exfiltration, manipulation, and destruction. For example, data manipulation can have life-threatening consequences when applied to air traffic control. The danger could not be detected in time. Finally, a real-life

adversary could extract a broad range of information from government computers, including personal data that could be used to his or her advantage, particularly in a politically dynamic place like Washington.

The results of *Eligible Receiver* were worrisome enough, but the fact that the simulators were severely limited in the scope of their attack should sound serious warning bells. The current national decision-making system is slow and cumbersome; defense and national information infrastructures are too interdependent and should be streamlined. As mentioned above, the system of oversight does not work when threats are fragmented across national borders. Moreover, the current "indications and warnings" process is simply inadequate and out of date. America has entered a horse and buggy into the Indianapolis 500 of information warfare, and runs the risk of being run down by more technologically advanced competitors before reaching halfway around the track.

It is important to build a national awareness that the threat to the American information infrastructure presents a serious national security concern. In February 1998, the issue was called to the public's attention by *Solar Sunrise*, a real attack on DOD computers. Two teenage hackers, with the help of an Israeli friend, explored the DOD computers and exploited the vulnerabilities they found. This is not fiction; the attack was real. *Solar Sunrise* was well publicized and completely separate from *Eligible Receiver*, although it did validate the findings of the prior study—government systems are vulnerable to attack. The more troubling part of the attack was that the media down-played the severity of the threat. For example, unknown security experts are quoted as saying that, "[t]he tools exist to defend the sites [if] people wish to defend them." Or, "most of the recent attacks have been 'ankle biters.' They're relatively unsophisticated efforts using easily available software that are more a nuisance than a danger." Or, "such 'security breaches' generally amount to nothing more than the equivalent of 'a kid walking into the Pentagon cafeteria.' If [the hackers] get into the war room, that's something different." If these sorts of intrusions go on every day, the United States is in deep trouble.

## IV. ENCRYPTION

Encryption can serve as a key defensive weapon in the battle to protect information. Unfortunately, our strategies are not yet well implemented, despite the known danger of terrorists, drug traffick-

ers, and others using encryption for their own interests. "Uncrackable" encryption is now available, and its possible entry into the marketplace where criminals have easy access generates legitimate law enforcement and national security concerns.

The division between overseas and domestic law enforcement is important to the American system of government and has served the nation well in the past. However, today's environment calls for closer coordination between the intelligence community, with its international expertise, and domestic law enforcement. MI6, the British intelligence agency, provides good reliable information throughout Britain. Britain confronts the unrest in Northern Ireland in many ways, including the intelligent use of good information. The United States has been clumsy about building the network between domestic law enforcement and overseas intelligence. To deliver good intelligence to American decision makers, the U.S. government needs to communicate the information better and quicker.

Without the capability of accessing encoded material through court orders and court sanctions, America will find it harder to fight the war on drugs, control terrorism, or ferret out racketeering. The matter of encryption is now before the U.S. Congress because the information technology industry collectively approached the appropriate committees asking for the authority to export encryption technology.

There are two additional components to the encryption debate: national security and law enforcement. Congress has recognized that there are two sides to the debate and asked the administration for a policy that addresses these security concerns.

Although strides are being made to address encryption issues domestically, the effort to bring international parties together on the issue has been stillborn. The French did not allow encryption for a long time, but have now begun to liberalize encryption regulation. The British are involved in much the same debate as the United States but are leaning toward more government regulation. Nations around the world are waiting for the United States to address the issue with a coherent policy. America needs a key recovery system or other technological solution. Whatever the device, it cannot be subject to abuse, since that would defeat the purpose of encryption protection.

The encryption question turns on the need for a single worldwide system, driven by commercial motivations. Business needs the benefit of an international network in order to compete. A large per-

centage of the business community will support a universal global policy, provided that the governments of the United States and Western Europe can get other nations to agree. Granted, there will always be freelancers who will strive to come up with a better product and peddle it off in the bushes to the mischief-makers. When legitimate law enforcement or national security purposes are apparent, and law enforcement is properly authorized to do so, governments should be able to decode encrypted material. Checks and balances could be incorporated in an international network in order to properly protect those who need protection.

People should not believe that government is able to decode all encrypted material. A system can provide the means for third parties to access plain text information, so that recovery is possible. If an uncrackable system is developed and only two people possess the key, the death of one of the keyholders poses a serious problem. With information assurance, the United States must address certifications and authorizations and determine whether the information has been tampered with. The encryption piece is the easy piece of the puzzle. If the U.S. government cannot resolve the encryption problem, it will be difficult to deal with the rest of the information dilemma.

Encryption has been on the legislative front burner for about nine months. The Security and Freedom Through Encryption Act has many co-sponsors; some sponsors have dropped out, upon realizing that encryption involves not just the Commerce and Judiciary Committees, but also National Security and Intelligence Committees. If encryption policy is studied carefully, it will be understood that there is more to the debate than responding to software vendors. Technological experts must find a way to preserve the protection of data, yet provide law enforcement with the means to get into plain text if necessary. The cause of the problem lies not in technology, but in ethics. The horse and buggy is about to be run over by the race cars.

## V. CONCLUSION

The growing importance of information technology presents not only new opportunities to benefit modern society, but also brings challenges to the approach and methodology of securing that society from outside attack. The form of threats facing the United States has changed and continues to do so; legislators and policymakers must shift their focus and dedicate resources and efforts to ensure that se-

curity measures are in step with evolving technology. The United States must not be the sponsor of the horse and buggy in the Indianapolis 500, guaranteed to finish last.