A COLLECTIVE SECURITY APPROACH TO PROTECTING THE GLOBAL CRITICAL INFRASTRUCTURE
A collective security approach to protecting the critical network infrastructure

This paper has been prepared by Dr Stephen Bryen, Managing Director, Aurora Defense: deltaone@aurora-america.com. A Collective Security Approach To Protecting The Global Critical Infrastructure is a "straw man" discussion paper on one possible approach to international cooperation in the area of cyber-terrorism and cyber-crime. This paper is one of a series of contributions to the ITU New Initiatives workshop Creating Trust In Critical Network Infrastructures to be held in the Republic of Korea, from May 20 to 22, 2002. The project manager for the Creating Trust In Critical Network Infrastructures initiative is Ivo Essenberg: ivo.essenberg@itu.int, working under the general oversight of Robert Shaw, ITU Strategy and Policy Unit. The opinions expressed in this report are those of the author and do not necessarily reflect the views of the International Telecommunication Union or its membership.
1 Executive Summary

Protection of the critical infrastructure from cyber attack is of great importance to modern nations. It is also important for global security and prosperity. In recent years, the threat posed has changed from what once appeared as an unstructured threat from adventurous hackers, to a structured, hostile attack on elements of the critical infrastructures of different countries. In some cases, governments and organizations with substantial resources are increasingly backing such attacks. To respond properly to this threat to security and prosperity, a strong, international solution grounded in a political framework is needed: isolated technical or legal solutions will not work. Moreover, efforts to confront structured hostile threats on a national level have been less than successful, and the technology employed has not been adequate to seal the systemic vulnerabilities in the information technology-dependent critical infrastructure. This paper argues that a collective security approach is needed to protect the global critical infrastructure.

1.1 Background

There is general agreement that communications networks are part of the “critical infrastructure” that is vital to national and international security. Increasingly, communications and networking services have begun an inexorable process of merger, as older analog services disappear and as communications rely on digital systems for voice, video and data connectivity. At the same time, as the user-base has expanded to include wider categories (governments, military, business, individuals), the increasingly merged digital network is becoming globalized. The digital networks of today are a collection of physical and switching and/or routing technologies (wireless and wired, copper, cable, fiber) providing access to systems, information resources and storage, technologies, organizations and individuals of every kind.

This emerging global communications network is a great force for modernization and industry offering access to a vast array of services. But it is also a point of entry and attack for criminals.

1.2 Network vulnerability

The vulnerability of computer and communications networks is well known—indeed, after the United States Department of Defense invented the ARPANET, the predecessor to the Internet, these networks have been constantly under attack. As knowledge about computers and networking has spread, and as standardized open systems replace proprietary architectures, attacking such networks has become easy work, even for amateurs. Where attacks are organized and professional, no network is safe (other than some highly classified networks not connected to the Internet).

A recent study1 of 4,900 computer professionals in 30 countries, found that there have been immense losses due to computer attacks. Virus attacks alone cost USD 1.5 trillion in 1999-2000. United States businesses lost USD 266 billion, or more than 2.5 per cent of GDP during the same period. The same study (supported by data from a Global Information Security Survey in 1998 and 1999) shows that computer “downtime” as a result of security breaches or espionage has been rising, with nearly 10 per cent of the respondents reporting downtimes of anything from 25 hours to 3 days.

The USD 266 billion figure represents the impact of viruses on US businesses with more than 1,000 employees, representing some 50,000 companies. If one also takes into account medium and small enterprises, the true impact of viruses on US businesses is much greater.

The fact that attacks are increasingly widespread and costly has promoted significant growth in the security industry. The Yankee Group forecasts that companies will buy USD 1.7 billion in security services by 2005, up from just USD 140 million in 1999. In 2000, Internet security software revenue has jumped 33 per cent to USD 5.1 billion. By 2005, this market will accrue more than USD 14 billion in revenue—a 2000-2005 compound annual growth rate of 23 per cent.

---

1 Information Week Research, July 2000
More indirect affects of computer attacks have included the removal of important systems from Internet connectivity as a security measure. Following the terrorist attacks of 11 September 2001 in the United States, for example, the Bush Administration directed Federal agencies to remove significant information resources from the Internet.

The problem is further compounded by the fact that, owing to connectivity, the locus of attack can be anywhere or everywhere at once. The disruption and confusion thus caused are therefore different from a conventional military attack, where the attacking force and its structure is generally known in advance. Thus, planning against a cyber attack differs in many respects from preparing a normal defence against a military threat.

This is, then, a unique situation: vulnerable, but vital global networks that can be assaulted from many locations simultaneously or sequentially and that, in any event, because of their structure and supra-territoriality, are hard to defend.

Solutions to this dilemma have so far been rather narrow and ineffective. Most attempted solutions have been localized, and system- or network-centric, in the sense that certain network “pipe” and “switch” operators have unilaterally built their own defences against attack. Unfortunately, because of dynamic change in the field of computers and communications, with near-continuous introduction of new technology, keeping up with defence of systems and network conveyance has been difficult, and requires discipline, knowledge and finances that are not always available. Where the main incentive is self-protection, and where self-protection can be interpreted in a variety of ways, the outcome in terms of broad network security is far from satisfactory.

2 Types of information warfare

It is necessary to distinguish between different classes of information warfare in order to reflect the fact that different segments of the network respond in different ways to this threat. For example, a major Internet service provider (ISP), or telephone network provider, may be concerned about privacy, particularly as protecting privacy affects their ability to keep customers. However, they may not be particularly concerned if a thief crosses their network to steal information or technology from an organization, or they may not perceive themselves as having a role in preventing terrorist attacks.

There are essentially three broad types of information warfare. Class I information warfare is about protecting privacy. Class II information warfare is about espionage, which can be against governments, corporations, universities, organizations and other structures. Class III information warfare is about terrorism, which includes cyber-terrorism, but which may also include attacks against other parts of the critical infrastructure.

Governments need to be concerned about all three classes of information warfare. But no government controls more than a portion of the global network, and there are no borders or boundaries that can be easily defended. Indeed, because many portions of the network are privately held, governments also have to elicit cooperation from the private sector. In the United States, the “voluntary” model for network and system security has been the preferred approach since the President’s Commission on Critical Infrastructure Protection (PCCIP) released its report in 1996.

3 Critical infrastructure

The PCCIP Report, and its subsequent implementation in the United States (based on Presidential Decision Directive 63 and subsequent executive orders such as the most recent Executive Order on Critical Infrastructure Protection in the Information Age of October 2001) all rely on independent financial support from the private sector.

The US Government has divided the critical infrastructure into the following segments: information and communications, electric power, transportation, oil and gas, banking and finance, water, emergency services.

---

2 http://www.info-sec.com/pccip/web/info.html

and government (including the military). These sectors have considerable regulatory capability, but as a matter of policy, all except government have been treated as voluntary entities for the purpose of network security. With regard to the government, substantial funds have been made available for network security and to counter cyber-terrorism. However, despite the availability of funding, the process of enhancing protection has moved slowly, with government agencies and the military departments continuing to struggle to formulate solutions that actually afford reasonable protection to the network.

The most ambitious and comprehensive plan is being implemented by the Department of Defense (DoD) and is known as DITSCAP (the Defense Department Information Security Certification and Accreditation Program). The idea behind DITSCAP is a comprehensive security evaluation of each DoD-owned or operated network, and the implementation of security measures to protect these networks. DITSCAP requires a thorough network review every three years, but it also requires that any important change to the network will trigger a review at the time the change is introduced.

Congress has also put in place a comprehensive security system for health care under what is known as the Health Insurance Portability and Accountability Act (HIPAA). HIPAA applies to the entire health delivery field (hospitals, laboratories, doctors practices, pharmacies, etc.). It requires training of all employees and a security plan to protect information (mainly patient records). Unlike DITSCAP, which is primarily focused on Class II and Class III information warfare, HIPAA’s focus is mostly on Class I information warfare.

HIPAA will be phased in over a number of years and is limited in its goals. DITSCAP is moving very slowly owing to the high costs and disruptions it causes in implementation, and the fact that the DITSCAP discipline, as good as it is, remains a relatively unproven commodity for network security.

3.1 Lack of success

Although the US Government is devoting billions of dollars to protecting military and government networks, generally it can be said that the results to date have been disappointing. The General Accounting Office (GAO) has consistently given failing grades to government organizations in implementing and protecting networks.

For example, in October 2001, Joel Willemsen, Managing Director of Information Technology for the General Accounting office, said recent reports and events indicate that efforts to beef up the cyber-security of federal systems are not keeping pace with the growing threats.

Willemsen noted that despite repeated reports chronicling many of the same vulnerabilities, critical operations and assets at many agencies continue to be highly vulnerable to computer-based attacks. "Despite the importance of maintaining the integrity, confidentiality, and availability of important federal computerized operations, federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk", he said. In August 2001, the GAO reported that "significant and pervasive weaknesses" might have jeopardized Commerce Department systems, many of which are considered critical to national security and public safety. In March 2001, the GAO said there continued to be serious security problems at the Department of Defense's Information Assurance Program.

Why is it that even with substantial funding available, and where the assets are under single national ownership (e.g. the government) that the defence of networks has been far from satisfactory?

The short answer is that defending individual networks connected to a global system is very difficult, because the source of the problem is beyond the reach of the individual network or even the government supporting the individual network. In military parlance, point defence is tactical, while the threat is strategic.

---

4 The house panel graded federal agencies on their computer security as follows: Social Security Administration: B; National Science Foundation: B; Education: C; State: C; Housing and Urban Development: C-; Commerce: C-; Agency for International Development: C; Defense: D+; Veterans Affairs: D; Treasury: D; Environmental Protection Agency: D; General Services Administration: D; NASA: D; Office of Personnel Management: F; Health and Human Services: F; Agriculture: F; Small Business Administration: F; Justice: F; Labor: F; Interior: F.

Note: Energy, Nuclear Regulatory Commission, Transportation, Federal Emergency Management Agency were received incomplete.

Source: The House Subcommittee on Government Management, Information and Technology.
4 Definition of the strategic threat

The strategic threat has the following characteristics:

- **The threat is structured.** A structured threat in this context means that some group, organization or government (or combination) is the source of the threat and is able to operate using a disciplined approach which includes the ability to assess the “enemy,” to measure the capabilities of the enemy to respond to an attack, to determine desired outcomes, and to coordinate attacks with political goals. For the most part, this marks the threat as different from “hacker” attacks, although some hacker attacks share characteristics with structured threats from organizations.5

- **The structured threat is well financed.** Governments and terrorist organizations have sufficient finances to buy equipment and provide various protective services to their personnel (for example, false identities), as well as operate from diverse locations in order to support their operations.

- **The structured threat is a hostile actor.** In this form of information warfare operation, the hostile actors are part of an organization with goals that are antagonistic to their target. Usually they have in mind a set of targets and specific operational goals. Unlike amateur attacks that are often thrill-based and transitory, structured, hostile actors are professional.

- **The structured threat protects its team,** thereby making it very difficult to roll up the attacking team. Unlike hackers, who can be tracked down and arrested, and who are vulnerable to some form of criminal justice, structured threat operators have a high level of protection.

- **The structured hostile threat is backed up by an intelligence agency or agencies.** This always applies to states and, in many instances, applies to hostile threat actors who receive support from states or who have sufficient resources of their own to operate an intelligence organ. Intelligence capability means the ability to field “insiders” who have access to sensitive networks; sometimes this means information provided from an agent, including countermeasures against the hostile threat. An example of such insider involvement is the attack on Citibank by a Russian “hacker” who was supported by agents inside the bank in San Francisco and in the Netherlands. An example of an agent is the case of Robert Hanssen, the FBI counter-intelligence special agent who was simultaneously in the employ of Russian intelligence services. Hanssen was an expert programmer with full access to all the sensitive computer systems of the FBI, Department of State and other government agencies. Concern about Hanssen was so great that, even after being put in jail, computer experts continued to search for Trojan programs Hanssen may have planted in sensitive law enforcement and intelligence networks.

- **The structured hostile threat may share information with terrorists or other countries** for a variety of political reasons. Thus, personal data about individuals, whereabouts of leadership elements, location of sensitive technology, military and financial data, even tip-offs about impending law enforcement operations, become valuable in themselves and can be sold or bartered.

5 It is also worth bearing in mind that hackers can be fronts for structured threats.

5 Countermeasures to the strategic threat

Most countermeasures are not designed to protect against the structured hostile threat, because developers of security protection systems and schemes do not fully understand the capabilities of such threats. In addition, virtually all efforts to put in place countermeasures are essentially one-dimensional tactical defensive solutions that are primarily based on limiting technical vulnerabilities.

Computer security protective schemes fall into the four following categories: **virus and intrusion detection; firewalls; vulnerability testing; and security patches.**

**Virus detection** is a means to test for viruses that may be introduced into a computer network or system. Virtually all virus detection systems are updated after incidents occur where the incident or incidents reveal a new type or “strain” of a virus. Some schemes include special heuristics to go after Trojan horse programs. Some viruses have the ability to both replicate and mutate, making them hard to detect and clean up. While
viruses are, for the most part, a kind of “nuclear weapon” against systems (some successful ones such as the “Love” virus caused widespread problems), they are not as dangerous as Trojans that may be buried in a system for long periods of time and activated by a hostile group by an electronic command. The good news about viruses is that the public always discovers them, though at some cost to the users’ systems. The bad news about the Trojan programs, is that they are more difficult to find, and no one is ever sure they have been liquidated. Trojans, like viruses, can migrate; some can even look up specific targets.

**Intrusion detection** (ID) seeks to identify and block attacks against a network. There are also variations on this theme, for instance: intrusion detection systems can be proactive and pursue the source of the attack. The key benefit of intrusion detection technology is that it works like a good biometric, revealing the *modus operandi* of the attackers. This alone makes intrusion detection systems, particularly the more sophisticated ones, highly useful for law enforcement. One of the main weaknesses of intrusion detection is that the detection system can be overwhelmed by false alarms. Professional hackers can blast a network or system and desensitize the human monitors. It isn’t uncommon for ID systems’ alarms to be shut off because they become a nuisance.

**Firewall** technology is a mature technology for preventing the misuse of certain ports and access points into networks. Technically located at a network gateway server, that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and to control any outside resources that its own users have access to.

Firewalls can be built as software or, to help protect them from attacks, firewalls can be produced in a combination of hardware and firmware. The key to a successful firewall is a consistent security policy and proper firewall configuration. One of the easiest, and most common, ways for an attacker to slip by a firewall is by installing some networking software on an internal system that communicates using a port address permitted by the firewall’s configuration. A structured hostile threat can be assisted by an insider ensuring that the firewall, no matter how good, will fail.

Virus protection, intrusion detection systems and firewalls are produced by private companies. While some of them have, from time to time, obtained support from government agencies, generally speaking they are commercial products. “Input” for the products usually comes from private and government computer emergency response teams (CERTS), but true intelligence support or cross-aggregation of information and data is still the exception rather than the rule. There is some international cooperation, particularly among university-based researchers and CERTS, but there is no strong intelligence support effort to back up these products. There are a variety of reasons for this lack of intelligence support; nevertheless, (as discussed further on) there are ways to overcome the objections, which are based on unwillingness to compromise sources and methods.

Unlike “active” measures such as virus detection or intrusion detection systems, **vulnerability testing** is a method used to test for weaknesses in a system. It is a form of system hacking aimed at revealing security vulnerabilities. Most vulnerability testing uses “scripted” attacks on a system. The “scripts” are usually classified into two forms: scripts that report on vulnerability but do not “challenge” the system; and active scripts, used where a real attack is mounted. Some security holes won’t show unless a real live attack is attempted; unfortunately such attacks can cause damage to a system that may outstrip the perceived value of the test. Proper vulnerability analysis requires a detailed roadmap of a network and the input of experts with experience in applying the scripted attacks. This is a controversial area owing to the risks involved in testing and the information that falls into the hands of the testers. Another problem is that, because systems are constantly changing, today’s vulnerabilities may not be tomorrow’s.

There are other, ancillary techniques for securing computer networks; perhaps the two most important are good security policies and adequate staff training.

---

6 For definitions of these terms, see the website: http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212964,00.html

7 For a definition of this term, see the website: http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci212377,00.html
6 Poor linkage in security protection schemes

Neither the technology (most of it privately produced), nor security policy and training, can be built in a vacuum. In particular, information about the threat is a critical component for improving security awareness and network defences.

Domestic solutions have suffered as a result of relatively poor linkage between the intelligence community (including both law enforcement and regular intelligence and counter-intelligence functions) and the inherent limitations of what tend to be national approaches in conceptualization of the situation and possible solutions.

According to this national view, the United States can independently solve the computer security problem by applying sufficient effort through formal and voluntary channels. This model has been in effect since the President’s Commission 1996 report, which devoted only one paragraph to international cooperation. But the model actually dates from 1988, with the passage of the Computer Security Act—the predecessor to the PCCIP—and the subsequent tasking of the FBI, the White House and creation of the Critical Infrastructure Assurance Office (CIAO). While there has been progress on law enforcement on the international front, and while the Department of State has run some outreach programs on critical infrastructure protection, the US approach remains predominantly national.

The entire framework (from the US perspective) can be summarized as follows:

- Funding for computer and network security for government agencies;
- Voluntary cooperation with the private sector;
- Limited international cooperation with the strongest effort in law enforcement;
- Most solutions developed by private industry (for both government and private sector) with minimal support from intelligence agencies or law enforcement;
- Weak data collection and aggregation.

7 The international alternative

An alternative approach might have the following elements:

- Improved international cooperation in setting technical computer and network security standards;
- Formal certification and accreditation system supported through international and national means applied to networks and to security products;8
- International coordination in intelligence gathering;
- International coordination in law enforcement;
- Agreed-on international benchmarks for measuring progress.

8 The Common Criteria system offers an attractive model for products.

8 The international framework

A key benefit of a global solution is that it can approach the problem of network security from an international political perspective. Thus, the possible range of solutions and options available to decision-makers is potentially much wider than nation-centric or local efforts to mitigate attacks.

To reach a global solution, a proper framework is required. This framework should consist of:

- agreement on a common critical infrastructure model;
- trust and confidence building between the participating countries and organizations;
- active government participation at the policy level;

8 The Common Criteria system offers an attractive model for products.
• a collective security approach.

9 Agreement on critical infrastructure

The notion of the critical infrastructure is an important starting point for cooperation among the industrialized countries.

As discussed, the US President’s Commission of Critical Infrastructure Protection delineated the United States of America’s approach to the concept of critical infrastructure. Nevertheless, the concept may have wider international validity, although some may want to broaden it to include certain essential industries. For example, in Japan, there is sentiment that a wide range of “administrative services” should also be classified as critical infrastructure, in addition to essential industries.9 Notably here also, there is a recognized need to find an international solution to critical infrastructure protection.

A fundamental feature of the critical infrastructure concept is that each part forms a vital element of national security. If the transportation sector is under attack, for example, as it was on 11 September 2001, then this can have a massive impact on the sustainability of the economy of the nation. Likewise, if the finance sector is severely disrupted, not only can it impact the entire conduct of business and government in a nation, but it may also impact other countries just as severely.

In the United States, efforts to “organize” critical infrastructure segments have largely been undertaken under a voluntary approach. The idea has been to provide forums and support for these sectors (e.g. banking, telecommunications) and to encourage them to develop their own standards for security. In some cases, such as the banking sector, this has been preferred because of the strong desire among bankers to avoid micro-management by government. The banking industry has always been highly sensitive to many of the information security risks it faces—particularly vis-à-vis reputation and public confidence.

In the US, as in most other countries, the majority of critical infrastructure is in private, as opposed to public, hands. While this may have been one of the reasons to tip in the direction of voluntary—as opposed to mandatory—security requirements, the voluntary nature of infrastructure security also relates to the fact that each sector needs to define solutions that are most appropriate to its own needs. For example, attacks on the banking system are far more common and persistent than attacks on the energy sector; and the nature of the attacks differ considerably.

In Japan, a good deal of attention has been devoted to studying the vulnerability of the manufacturing sector, and particularly the vulnerability of oil refineries, which are essential to manufacturing and transportation. Japanese specialists have thoroughly evaluated oil refinery security and particularly the possibility of attacks on the control systems in refineries, which is a main point of vulnerability. It can be said then, that Japan has developed an important capability and experience that might be shared among other nations seeking to protect oil refineries from cyber-attack.

What is true of civilian infrastructure is also true for the military infrastructure. Today’s military operations require huge amounts of telecommunication and computer network bandwidth. Much of this bandwidth has to be allocated from civilian communications networks. Over 60 per cent of military communication services and over 90 per cent of surge communications are expected to be commercially based by 2010. Indeed, this demand for bandwidth will increase even more if new plans for military units are implemented. The age of the cyber-soldier and the military robot will be fast upon us.10

It is important to note that this not only implies that the civilian infrastructure must be reliable and robust, but it also means that the military units will also typically need to be interconnected with other “coalition” partners from other nations. Recent conflicts such as the Gulf War, Bosnia, Yugoslavia and Afghanistan all point this way and make clear how vital international connectivity and inter-networking trust are. Therefore,


10 In the wake of the 11 September events, the “number one” technology challenge facing warfighters in Afghanistan was the need for more bandwidth, said Air Force Major General Charles E. Croom, Vice Director for Command, Control, Communications and Computer Systems with the Joint Chiefs of Staff. “It’s always bandwidth,” Croom said, noting that the Department of Defense’s bandwidth need has increased steadily since the Gulf War. “The demand always outruns the capacity.”
A collective security approach to protecting the critical network infrastructure

in the case of the military portion of the critical infrastructure usage, trust and connectivity as well as robustness and reliability are key requirements for success.

10 Trust and confidence building

While it would seem that there is a strong basis for the advanced industrial countries to combine their efforts to put an end to cyber-crime, some serious barriers stand in the way of doing so because of competitive and political differences among industrialized nations.

One obstacle is the use of the communication networks, which includes the Internet, for commercial and political spying. For example, the European Community has complained bitterly about a program called Echelon. As the European Parliament reported, “Europe wants to become the most competitive and dynamic knowledge-based economy in the world. A pre-condition to achieve this is the need to build trust in electronic communications.” In criticizing Echelon, the European Parliament stated: “The abuse of large-scale communications intelligence is something that can make an individual living in a democratic society feel uneasy. Privacy is a fundamental right. Any derogation from this right has to be specifically provided for by law, necessary for objectives of general interest, proportionate, and subject to adequate checks and guarantees against any form of misuse.”

While Echelon has been singled out as an example of how the Internet can be used for spying by some nations (namely, the United States of America, United Kingdom, Australia and New Zealand), the fact is that many, if not all, countries are increasingly using the Internet for intelligence means. The question is where does “spying” on the Internet cross a barrier of acceptability? If, as has been claimed in defence of Echelon, the “spying” is actually the gathering of “open source” information which is “public” in character, then can such a system be characterized as “spying” or merely as a breach of trust?

This is quite a complex and contentious issue, and spying that is legitimate to national security compounds the matter. For example, the terrorists of 11 September 2001 and Al Quaeda are known to have used e-mail and Internet communications to coordinate attacks in the United States and other countries. Even more recently, the journalist Daniel Pearl of the Wall Street Journal, who was murdered by Al Quaeda-linked sympathizers, was tracking some of those e-mail communications. Ironically, his alleged killers, who believed they were using anonymous e-mail facilities, were tracked down through an Internet address embedded in an originating e-mail message header.

While few would deny that it is legitimate to pursue terrorists and that, if terrorists use the Internet for their plots, then it is proper to use the Internet to hunt them down, there are many murky areas where law enforcement comes into conflict with human, political and democratic rights of speech and privacy.

Ironically, the events of 11 September 2001 have given rise to better understanding among the industrialized countries—at least with respect to international terrorism—and thus to an improved atmosphere in which to try to establish ground rules for future conduct. This work is essential, because the importance of network security to economic growth and prosperity is unquestionably at stake. It follows that a global approach to critical infrastructure security will help set proper boundaries and promote a common vision of security that will be sufficiently robust and clear while also protecting privacy and democratic rights and freedoms.

That said, neither osmotic processes nor luck are likely to bring about successful results. The path to rebuilding trust and confidence will take enlightened high-level leadership and a willingness to set reasonable operational boundaries. Hammering this out will not be easy.

11 Collective security

One example of a collective security system has been the North Atlantic Treaty Organization (NATO) and its military arm SHAPE (Supreme Headquarters Allied Powers Europe). Only France, although a member of NATO, is not a member of SHAPE.

As a collective security organization, the premise of NATO is that an attack on one country is an attack on all and therefore NATO will respond on behalf of all member countries (currently numbering 19).

While NATO emerged as a result of World War II, it quickly defined itself in terms of its view of its primary adversary at that time, the Soviet Union, and the Warsaw Pact alliance. NATO always thought of itself, until
the break-up of the Soviet Union, as primarily concerned on a massive attack that, it was expected, would involve nuclear weapons. Thus, NATO focused heavily on deterrence and organization to prevent such an attack. In the early days, this included countering Warsaw Pact nuclear threats by deploying nuclear assets (nuclear howitzers, mines, and the Nike-Zeus missile defence system) and deploying military units in critical areas (e.g. Germany, Belgium, Italy, Turkey).

Any massive attack was relatively easy to define, and NATO’s response was carefully planned and calculated. It was regarded as important to make sure that the opposing force understood the depth of counter-force planning, the nature of the military doctrine, the coordination of the various allied forces, and the coherence of the alliance. Together, these elements formed what planners called *strategic transparency*, so there was no confusion as to the possible consequences or automaticity of response.

Is it possible to apply such concepts to defence against cyber attack? If the key proposition of NATO might be summarized as “an attack against one is an attack against all” and the correct response would be that each state is obliged to come to the defence of the others under attack, then one could envision an analogous formula for cyber-attacks: any attack against an agreed element of critical infrastructure would be considered an attack against all, and the parts of the collective security arrangement would be obliged to provide all possible assistance to combat the attack.

In this case, one can foresee that all possible assistance would include sharing intelligence, mounting a common enforcement effort to go after the source, or sources, of the attack and to continue to respond until the problem is resolved. Of course, this involves a very high level of advance coordination and planning.

In fact, planning and coordination are extremely important because of their value as a deterrent. Planning needs to be carried out by an organization that has real tangible response capabilities with potential consequences for the attacking party. Without prejudging the steps the planning group would wish to implement, one can foresee a series of steps that might include severe sanctions against states that allowed attacks to be mounted from their territory or that refuse to cooperate in halting the attacks if they came from non-government sources.

There are considerable advantages to be gained from this approach. A particularly important advantage is that the usual distinction between the “independent” hacker and the professional would be rendered meaningless. Rather, the meaningful role emanates from the threat the international alliance can bring to bear against those who would disrupt or damage the critical infrastructure. If a serious attack is mounted against the critical infrastructure of one of the member countries, then the others—under a pledge to respond—would set in motion a series of actions and potential sanctions which the offending state would have to face. If the root cause was a teenage hacker, this would be of no real consequence to the affected nation, as it would be obliged to shut down the attacker in a manner that would satisfy the alliance countries. For the first time there would be concrete and demonstrable incentives for action against the source or sources of attack.

For such a system to work, like other collective security arrangements it would need to have a concrete structure and be properly formalized as or, alternatively, chartered through a treaty organization. It is doubtful that more informal cooperative models would be applicable to this problem. The Coordinating Committee for Multilateral Export Controls (COCOM) might be an example of this type of model.

COCOM (1949-1996) was a cooperative international initiative spun-off from NATO. Originally part of the military embargo of the Warsaw Pact countries, headed initially by an Italian Admiral, COCOM became an unofficial and secret operation intended to continue the embargo on goods and technology. COCOM had its own charter, but it depended totally on the goodwill of members to implement the COCOM programme. Most of them did, which included implementation of sanctions against their own citizens who may have violated the embargo. But the COCOM system, as it evolved, worked largely because it always was a sort of adjunct to NATO, although it included at least one quite prominent non-NATO member, Japan.

The main weakness of the COCOM system was that it was not a collective security system, although in a derivative sense it reinforced the NATO collective security alliance. Also, COCOM could not and never did impose any sanctions on other countries, although in the opinion of the Soviet Union and other Warsaw Pact countries, as well as China and North Korea, the very fact of COCOM’s existence amounted to sanctions. In fact, from that perspective it was a long-lived sanction that ran for 47 years and, that effectively even continued after COCOM’s dissolution in the form of national licensing systems that maintained limits on
national security technology which could be sold to Former Soviet Union (FSU) countries, North Korea and China. Thus COCOM’s lifespan effectively extended to more than half a century.

COCOM also lacked official military representation—a fact of some importance, as the main purpose of the alliance was to reinforce the national security of the member countries. Some countries—the US, UK and France—generally included military experts in COCOM meetings, but Foreign Office or trade representatives typically led all COCOM delegations.\footnote{In response to pressure from the US, an outside organization was formed in 1987 which was made up of military “experts.” Because of Japan’s particular situation, Japan’s military experts came from the Prime Minister’s office and not from Japan’s Self Defense Force. The military experts group had a separate secretariat that was led by a French military officer, and the group conducted its studies from offices supplied by the French Government.}

An interesting fact about COCOM was participation by private companies. In principle, government officials always led COCOM, and governments funded its secretariat. But various delegations often brought experts from the private sector to assist them in defining key parts of the COCOM export control lists. Private sector individuals who were lent to the national government for the purpose of serving as COCOM delegates headed certain delegations, as was the case for the Danish delegation. While there was a propensity for national delegations to favour their most important private companies in the list reviews, the presence or absence of private sector representation did not make any particular difference, other than in the depth of knowledge about the industry in question.

An organization without a strong government presence, or representing only a part of any government, would not be effective. A good case in point is law enforcement. It might be thought that coalitions of law enforcement agents from different countries could, in isolation, sort out what needed to be done in the law enforcement field. In fact, this is already happening to a certain degree, and while it helps to catch and prosecute the occasional felon, it lacks the political response essential for the successful protection of the critical infrastructure.

A treaty organization, or the juridical equivalent, would be a powerful political statement by governments that they have in effect lent some part of their sovereignty to others in return for an improvement in collective security.

Would a political level treaty on the subject of infrastructure protection be possible? This would depend on a realistic forecast of its operation and activity, and testing its efficacy in a step-by-step implementation programme. Such a step-by-step programme would accomplish two goals: it would initiate a planning effort and help establish whether strategic planning is possible in this field, and it would be productive in halting aggression against the critical infrastructure by allowing the member countries to test the system against a specific part of the critical infrastructure to see if it worked.

The following are some candidate elements of the broader critical infrastructure.

- telecommunications backbone (voice, data);
- banking and financial markets;
- health and emergency services;
- transportation systems;
- critical manufacturing;
- energy and water
- government services
- military

It is probably most important to focus on the first and the last elements in the list.

Telecommunications are what the critical infrastructure lives off, and thus play a role that is vital to all the sectors. Protecting this sector is, therefore, an important way to protect the others—at least in part. This “industry” has many sub-segments (land base, wireless, satellite, underground and underwater, etc.). It is an
area where a lot can be done to provide a high level of protection, and where agreement on security standards can significantly enhance security and thwart attackers.

The last category, the military, is closely linked to telecommunications, and increasingly so as, what is known in the United States as the “Revolution in Military Affairs” (RMA), continues to grow.\textsuperscript{12} Because of the military reliance on computer networks and military as well as commercial carriers, the robustness and availability of communications is of great importance. So too is the ability to link different networks together among international coalition partners. In that regard, NATO already has a number of pilot programmes, as does the US Department of Defense, to test ways and means to certify and accredit networks that can be linked together at times of coalition stress or military emergencies.

While it may seem that building trusted networks is a purely military matter which lies outside the framework of an international organization, in reality this is hardly the case. In fact, the military networks heavily use commercial networks and thus are easily exposed to network attacks launched on public infrastructure. Unless the military can operate secure networks entirely in isolation and not use any commercial equipment, they are equally exposed.

In fact, the degree of exposure to risk is much greater than ever before, at least in the US military, which is among the most advanced in applying new technology. In the early 1990s, the US military decided to strongly encourage the use of “COTS” technology. COTS stands for “commercial off-the-shelf” technology. Instead of buying “gold plated” custom systems, the Defense Department promoted the widespread purchase of COTS equipment, even going so far as to end long-term programs including TEMPEST.\textsuperscript{13} One driver in the use of COTS was the rapidity of the technology cycle and the perceived need to field the most modern equipment possible. Another driver was a wider enthusiasm for the RMA.

With a move to COTS and away from military-proprietary software\textsuperscript{14}, the US and allied military began to deploy systems that were vulnerable to the same types of attacks and hacking as commercial systems. While COTS clearly offers certain advantages, it is also potentially dangerous for three reasons, namely: first, almost all COTS hardware and software platforms have an “open architecture” design in order to facilitate linkages between different hardware formats and applications; second, virtually none of the COTS platforms was designed around coherent and disciplined security standards, and thus most of them were “born” with very large security “holes”; and third, knowledge of the systems is widespread and experts can be found in both developed and developing countries. The international knowledge base has been broadened by access to low-cost markets for programmers. Little attention—if any—has been given to the political or military consequences of this spread of knowledge.

The use of open systems by the military raises the question of whether there is any role to be played by a civilian organization in protecting such systems.

There is more than one answer to that question. In wartime, if cyber-attacks originate from a hostile state it is obvious that there is little help that can be provided beyond what the military itself can do against the enemy. But if, during wartime, the attacks originate from a non-hostile party (even if only their territory is being used for such purpose), then a well-run international organization intent on protecting networks from attack

\textsuperscript{12} The *Revolution in Military Affairs* (“RMA”) is defined as a broad change in the structure and operation of the United States defence “system.” RMA is linked directly to rapid changes in technology, particularly technology prevalent in the civilian economy and the potential to exploit these technologies and enhance the effectiveness of America’s defence forces. RMA—in many of its applications—relies on commercial networks such as telephone switching systems and computer networks, with the Internet being an increasingly dominant factor, and transmission platforms such as microwave links, under-water fiber optic lines, satellites. etc. Disruption of any commercial network is, increasingly, a national security problem as well as an economic concern. Because of the computerization of power transmission grids and other utilities, and the reliance of air transport on wide area networks and computers, sophisticated adversaries can disrupt knowledge.

\textsuperscript{13} TEMPEST was a program to electrically shield equipment so that it would not broadcast or emanate information. TEMPEST was applied to computers and ancillary equipment.

\textsuperscript{14} In the mid-1980’s, the DoD mandated the use of the ADA programming language. ADA never gained popularity in the commercial sector, which evolved from programs such as Cobal and Fortran to C and C++ as common programming languages. While ADA was optimized for real time and rapid conversion of analog to digital information, much faster microprocessors and digital sensors circumvented most of these advantages.
A collective security approach to protecting the critical network infrastructure

can have an impact. Finally, during periods of peacetime, the same international organization can play a very useful role in keeping networks clear of attacks.

Based on all the determinable evidence, the trend towards using civilian communications systems in support of the military infrastructure, and to use COTS systems, will continue and will probably expand. This would tend to support the argument that, along with considering how to protect the telecommunication infrastructure, a quite parallel course of action should be employed to protect the public side of the military telecommunication and network infrastructure, which is in any case embedded in the civilian network.

12 Postulating an international organization

Based on a premise that it makes sense to have a treaty-based (or near-treaty-based) organization to combat cyber-terrorism and cyber-crime, the question needs to be addressed of how such an organization would be structured and managed. For the purposes of this discussion, a hypothetical model of such an organization, to be called “the Cyber Security Coordinating Organization” (CSCO), is described below.

The following are the critical elements of CSCO, including an approximation of the funding levels required.

The members: There would need to be a clear collective standards for admission. Aside from the states represented, the composition of each delegation also needs to be defined. It is suggested this be composed of a high-level political representative, probably of ambassador or assistant secretary rank, supported by key government agencies. It is important to stress the political character of representation; while the organization would certainly have a technical aspect, the purpose is not to promote any one particular technical solution, but to formalize a political will to put a stop to cyber attacks.

The charter: CSCO would need a proper charter that would reflect as its most important element the collective security nature of the undertaking. The charter would have to be approved by states and ratified if the treaty approach were followed.

The secretariat: Functioning international organizations need a Secretariat to operate efficiently. This implies the requirement for a Secretary-General, or equivalent, to head CSCO. Particular attention is needed to ensure that both the Secretary-General and the staff do not merely perform bureaucratic duties. Therefore, the Secretary-General should be someone who has previously held a high national rank, either as a Cabinet Secretary or in a senior military post. The job should be fixed term (four years, for example) and compensation should be based on the salary of the previous post in government plus necessary expenses.

Costing the operation of a secretariat is not simple. COCOM operated with a staff of about 20, and a budget that never exceeded USD 5 million. Its physical plant in Paris was contributed by the US Government (it was an annex of the US Embassy, although located some distance from the Embassy building). In general, a budget in the order of USD 10 million would probably constitute a good initial budget for such an organization (providing that most of the member nations contribute personnel and provide other in-kind assistance).

A key role of the secretariat would not only be to set the agenda for the CSCO, but also to function as a policy review organization for the organization. The secretariat would be responsible for organizing regular and special high-level meetings. The high-level meeting would be a voting body and would have the authority to admit new members, to approve the accrediting of networks, and to deal with violations—including the ability to recommend the imposition of sanctions.

In order to obtain charter approval, it is likely that a voting scheme would have to be agreed on, particularly for the most sensitive issues (sanctions, membership). Whether this should be by unanimous approval (e.g. as COCOM followed), or some other formula, would need to be agreed on.

A related issue is that of secrecy. In order for CSCO to pursue cyber attackers, it would have to be privy to sensitive information. NATO has such a scheme in place; and COCOM was able to handle classified information. The new organization would have to be granted some form of clearance from member governments and would have to be managed so that the information could be safeguarded. Even with clearances, it will take time to build sufficient confidence in the organization to enable sharing of really sensitive information.
12.1 Beyond the secretariat—the organization

Once the secretariat was staffed and the high-level meeting process put in place, CSCO would need to be organized in order for it to operate properly.

To this end, the following centers are proposed:

- **Cyber warning center.** The purpose of the cyber warning center would be to afford a means to coordinate intelligence related to possible cyber attacks and provide a conduit to warn governments that such attacks may take place. What marks the cyber warning center as different from the private sector is that it would be able to operate on a secure basis with classified information that is available to member states. It would be a larger form of the US Government’s proposed Cyber Warning Information Network. For the cyber warning center to operate, it would need to have secure links to the member countries and some means of functioning outside the Internet (e.g., perhaps through dedicated lines). This would be a type of “hotline” system. For operations, it would coordinate with CERTs (Computer Emergency Response Teams) and other public and private groups as appropriate, and within the limits imposed by the confidentiality of information and security.

- **Legal affairs coordinating center.** The legal affairs coordinating center would attempt to focus and centralize the various law enforcement initiatives already under way in the international community. The chief advantage of a central, international coordinating center within the framework of a collective security system would be that the forensic and prosecutorial work of the law enforcement community would also translate into policy action relevant to network protection equities. Thus, the work would inevitably be broader than trying to capture lawbreakers or focusing on standardizing the legal framework of enforcement against cyber crimes. But it would be a mistake to believe that this center could be effective or function smoothly unless it were made up of legal and police experts and practitioners. A related benefit is that the center could propose legal standards that could be approved by the high-level meetings of the larger organization. Just as in COCOM, the List Review process resulted in setting a framework of rules and regulations for COCOM member countries (even though this was never formalized), in this context, determinations about legal standards in the framework of high-level meetings would be of special importance to the member countries, perhaps enabling some of them to adopt guidance from CSCO.

- **Business and industry cooperative forum.** The critical infrastructure is, in functional terms, the province of business and industry, whether the business and industry is owned by the state, by municipal government, or privately held (by public or private owners). The work of CSCO could not be effective without cooperation from, and consultation with, affected business and industry. In general, the US experience with “voluntary” cooperation has demonstrated improvement in overall cyber-security, particularly in respect of the development of standards. In this connection, there has been important international progress in the International Organization for Standardization (ISO) in establishing an overall security standard, derived from British Standard BS7799. The UK Government sponsored the development of British Standard (BS) 7799—Code of Practice for Information Security Management, which, as of 1 December 2000, has been published as the International Standard ISO/IEC 17799:2000. ISO/IEC 17799 aims to allow compliant companies to publicly demonstrate that they can safeguard the confidentiality, integrity and availability of their customers' information. The standard provides over 127 security guidelines structured under ten major headings to enable companies to identify the security controls which are appropriate to their particular business or specific area of responsibility. As well as giving detailed security controls for computers and networks, ISO/IEC 17799 also provides guidance on security policies, staff security awareness, business continuity planning, and legal requirements. On the basis of ISO/IEC 17799, it should be possible to delineate specific standards for critical infrastructure segments. There would be (at least) three important benefits for the Business and Industry Cooperation Forum in doing so. These are: first, standardization of security, which is an essential step in isolating points of weakness and finding defensive solutions; second, establishing network trust and trustworthiness, which is fundamental to CSCO’s objective, and third, providing a way to certify and accredit networks for security. Quite possibly, the complete methodology for security compliance might be made available only to member countries and to companies and organizations that are part of the critical infrastructure and are at an inherent trust level to receive such information pertaining to
methodology. This would, to some degree, diverge from current practice, which consists in debating and publishing security manuals and guidelines for public benefit. One problem is that such debate and publication also provides a detailed road map to the “bad guys”, enabling them to pick out shortcomings in the plans and methodology and seek to exploit vulnerabilities. However, if inside the framework of CSCO there were a “Business and Industry Cooperative Forum” drawn from the affected critical infrastructure companies and organizations, it might be possible to carry out the highly detailed security planning in a more secure atmosphere. This, in fact, is more consistent with standard security practices in NATO and in many governments.\(^{15}\)

- **Technology security committee.** Although the aim of CSCO would be to raise to the political level an organization capable of dealing with national security and global security threats, it would need a body where technical security information could be exchanged. The intention is not, however, to replace any of the numerous currently existing approaches to processing technical security information. However, government agencies in the United States, the United Kingdom, France, Germany, Japan and elsewhere are investing heavily in trying to develop innovative security systems. One issue is how to share these, as well as to evaluate their applicability and effectiveness. In the United States, for example, the Defense Advanced Research Projects Agency (DARPA) is sponsoring considerable research in network protection. Some of the outcomes of the research are likely to prove valuable. Likewise, a number of governments are cooperating in a programme called the “Common Criteria”, a scheme whereby hardware and software can be ranked for their security value. The Common Criteria is now an ISO standard (ISO/IEC 15408:1999) and a “mutual recognition arrangement” (MRA) is in place. The MRA facilitates the acceptance of evaluation certificates awarded in one country, to be accepted by another. Above all, the Common Criteria system shows that it is possible not only to share technical security information, but also to provide a means for recognizing the certification and accreditation work carried out in the different participating countries. In the long term, if widely accepted, Common Criteria could be a way to improve on hardware and software security vulnerabilities and will help mitigate the pure reliance on COTS. Considered holistically, the work of the technical security committee would form an important backbone and supporting structure to the work of the Business and Industry Forum.

13 Conclusion

This paper has attempted to show that, while a good deal of important work on security has been carried out internationally in a wide variety of forums, efforts so far have fallen short of a formal international treaty approach to the problem. The key benefit of such an approach is that it represents a political means to combat a problem which is threatening the critical infrastructure of many countries and which, ultimately, may undermine collective global security and peace.

In the context described here, the collective security model— in the form of a treaty organization—is an appropriate response to a structured hostile threat from cyber-terrorists. In today’s environment of increasingly interconnected global network systems, the framework described above bears the essential features that such an organization would need to have if the problem of structured cyber-terrorism is to be

---

\(^{15}\) One of the unusual aspects of IT security is that it has been almost entirely treated as a public domain issue. This may have been an acceptable practice when the overall threat was from hackers and was unstructured and, quite possibly, not fundamentally hostile. However, attacks on computer networks today are more likely to originate with the backing of hostile governments. The threats are therefore far more structured and operate with greater resources than hitherto. In these circumstances, the proper way to respond is to have an equally structured framework for defence of infrastructure. For such a structured defence to work, its fundamental integrity has to be assured. This is not easy when large segments of the infrastructure are managed by business and industry and not by governments. A disciplined, tightly contained, set of security measures is therefore of great importance for success. Consider, for example, the use of encryption as one component of a security strategy. It does not make sense to declare in advance the encryption algorithms used, key lengths, software and hardware and other “heartbeat” information about system security. Consideration needs to be given not only to protecting such information, but to making sure that contractors and vendors involved in supporting the critical infrastructure protect the information too. In the United States there is growing concern about the “origin” of security software, as the trust factor is very important. If proper security practices are not implemented at the international level, for example in the form of the proposed CSCO, then one natural (but not satisfactory) resource would be to draw hard lines around domestic parts of the infrastructure that are deemed vital to national security. This would result in a trend towards more closed systems at a point in time where connectivity (not necessarily openness) is important.
successfully challenged. For nations to adequately protect their critical network infrastructures in the future, there is doubtless a need to consider such a collective approach as the way forward.