NATO and Cyber Defence

Mission Accomplished?

Rex B. Hughes

What steps have been taken by NATO against the threat of cyber attacks? What needs to be done to prevent them in the future?

Nearly two years have passed as of this writing since a massive electronic attack identified as denial of service (DOS) temporarily crippled Estonia's national Internet infrastructure.[1] From the perspective of NATO the attack was an historic moment in the evolution of the Alliance because it represented the first time that a member state had formally requested emergency assistance in the defence of its digital assets. As the attack escalated over a period of weeks, NATO ministers met in haste to grapple with the strategic and political consequences of the first major cyber attack on a member state. During the crisis it became patently clear to NATO officials that the Alliance lacked both coherent cyber doctrine and comprehensive cyber strategy.

Cyber Bucharest

The 2008 NATO Bucharest Summit marked the first time the Alliance grappled with the cyber dilemma within a formal summit framework. At a private workshop concurrent to the Bucharest Summit, Romanian President Traian Băsescu introduced a series of working papers, including one on NATO and cyber defence. During the Summit NATO officials and cyber experts reviewed the lessons learned from the Estonian experience. Section 47 of the Bucharest Summit Leader's Declaration stated that:

> NATO remains committed to strengthening key Alliance information systems against cyber attacks. We have recently adopted a Policy on Cyber Defense, and are developing the structures and authorities to carry it out. Our Policy on Cyber Defense emphasizes the need for NATO and nations to protect key information systems in accordance with their respective responsibilities; share best practices; and provide a capability to assist Allied nations, upon request, to counter a cyber attack. We look forward to continuing the development of NATO's cyber defense capabilities and strengthening the linkages between NATO and national authorities.

Now that nearly a year has passed since the first NATO head of state declaration on cyber defence and with the approaching 60th anniversary summit, it is time to review what NATO both has and has not accomplished in the rapidly evolving cyber domain.

As of this writing there have been two major post-Bucharest deliverables, one operational and the other strategic.

1. NATO Cyber Defence Management Authority (CDMA)

On the operational level the creation of a new Cyber Defence Management Authority in Brussels represents a bold effort to centralise cyber defence operational capabilities across the Alliance. According to NATO's public affairs division, the Brussels based CDMA will augment member cyber defences by providing a centralised bureau for

coordinating member responses to the full spectrum of cyber attack. While there has been little information shared about this authority's precise capabilities, it is thought to contain advanced real-time electronic monitoring capabilities for pinpointing threats and sharing critical cyber intelligence in real-time. During the next few years the CDMA is expected to evolve into a war-room operation for NATO's cyber defences with actual tactical responses carried out by member states through a 'coalition of the willing'. Unlike during the attack on Estonia, member states now have a number 'to dial' during an actual cyber emergency.

2. Cooperative Cyber Defence (CCD) Centre of Excellence (CoE)

The second post-Bucharest deliverable is the Tallinn based Cooperative Cyber Defence Centre of Excellence. Seeking to reverse its cyber victim status, Europe's most wired nation took the lead in establishing NATO's first cyber centre of excellence.[2] Whereas the CDMA is charged mainly with coordinating NATO's cyber defence in an operational capacity, Estonia's CoE will advance the development of long-term NATO cyber defence doctrine and strategy. Established formally in May of 2008 and receiving full NATO accreditation in October of 2008, NATO's CCD CoE has begun to explore how the Alliance can strengthen its cyber defence capability for the long-term. As indicated via its website, the Cooperative Cyber Defence Centre of Excellence has planned a series of events and workshops to seek input from a range of public and private actors both within and outside of the formal Alliance structure.

Steps to Be Taken

While NATO is to be commended for taking concrete steps on both operational and strategic levels, there is still much work to be done.

1. Computer Emergency Response Teams (CERT)

One area that warrants more attention by NATO members is the creation of national CERTs. The CERT concept was pioneered in 1988 by the Carnegie Mellon University in the United States. At the time, Carnegie Mellon researchers determined that a growing number of network intrusions required a centralised emergency response team to deal directly with threats in real time before these escalated into national-level emergencies. Today, there are over 250 operational CERTs worldwide although a few NATO members still lack fully staffed national CERTs. Since 9/11 the U.S. and other leading economies such as the United Kingdom have worked to create state sponsored CERTs to coordinate cyber defences at the national level. Following discussions in Bucharest and in other NATO ministerial meetings, it is generally accepted as an advantage to the Alliance for all NATO members to establish national CERTs although no formal recommendation has

NATO's Cyber Defence Management Authority is expected to evolve into a war-room operation for NATO's cyber defences. Pictured are U.S. electronic warfare officers at Eglin Air Force Base, Florida (Photo: U.S. Air Force Cyber Command/C. Kessler) been made. If the CDMA is to be effective at both gathering intelligence and mobilising cyber assets, it is vital that all Alliance members commit to creating national level CERTs that are empowered to share information and assets during any severe cyber attack as carried out against Estonia and more recently during the Russian aggression taken against Georgia.

2. International Law

One major issue in particular that needs to be addressed within the cyber domain is the role of international law. To date there has been little public discussion within NATO on what role, if any, international law should play in governing either offensive or defensive cyber actions. There are few treaties or UN statutes that deal explicitly with cyber actions.[3]

One possible explanation for the lack of a coherent international legal framework governing cyberspace is that great power states such as the U.S., China, and Russia may desire a significant degree of strategic ambiguity while they shape their own national cyber based military capabilities. Another possible explanation is that too few diplomats and legislators lack the requisite technical expertise to comprehend fully the scope of cyber defence issues. NATO's Parliamentary Assembly is one such body that is poised to begin deliberating on the international law issue, but to date few parliamentarians have demonstrated any credible leadership on cyber issues. However, this attitude will likely change as more tech savvy Generation X and Y leaders assume higher office in NATO member states. While NATO membership defined within the Euro-Atlantic community limits the scope of the Alliance's global authority in cyberspace, NATO's status as the preeminent international military alliance provides sufficient legitimacy to begin articulating a global vision for a constitutional cyber order. NATO should take action on this issue in 2009 and the CCD CoE is well positioned to explore the creation of a cyber *jus in bello*.

The creation of a cyber jus in bello should be explored

Harmonisation of national and international codes, regulations, or laws is an ever present challenge. National criminal laws may cover intentional falsification, unauthorised access to stored information, privacy, credit and financial information, industrial espionage, and major network intrusions. Violations would prohibit a military response until the culprit is identified or assistance is requested by the national investigative or policing body, such as the U.S. Federal Bureau of Investigation (FBI) or the UK Serious and Organised Crime Agency (SOCA). In the United States, if the culprit is determined to have been a foreign source, the investigation would involve the Central Intelligence Agency (CIA) while financial intrusions would usually fall under Secret Service authority. MI5 is charged with investigating threats to UK national security.

If cyber defence is basically a national responsibility, what may NATO member countries legitimately do under a range of laws – international law, armed conflict law, telecommunications or satellite law, and criminal law? What will actually or legally become the responsibility of the NATO command? U.S. Major David J. DiCenso, writing in the *Airpower Journal* (Summer 1999), succinctly summed up the range of legal issues as information warfare is increasingly thought about and talked about in the real world of computer-aided global communications.

Recognition of the 'customary laws' of nations form much of international law, as DiCenso was careful to explain. Thus, the Law of Armed Conflict already exists and the same principles would apply to what he calls the "cyberspace battlefield", where both combatants and non-combatants are protected. Defining the scope and severity of the damage definitely presents challenges for domestic and Allied commands. How will NATO accommodate the realm of the major Western alliance with the realm of criminality and enforcement under international laws? During the last decade, there have been discussions about amending the laws of war to include cyber attacks, but no country or group of countries had seriously pursued this line of thinking. Instead, countries had found mutual benefit in a *status quo* of strategic ambiguity. However, the potential for the United States and other leading powers to transform cyberspace into a premier 21st century war-fighting domain may prompt lesser states to champion an international cyber defence treaty framework that would more clearly delineate acceptable practices in modern cyber warfare.

3. Global Partnerships

At the Bucharest Summit, the concept of Global Partnerships earned a prominent place on the agenda and will likely command significant attention at the 2009 Franco-German Summit in Strasbourg-Kehl.

> We value highly the contributions that our partners are making to NATO's missions and operations. Seventeen nations outside the Alliance are contributing forces to our operations and missions and many others provide different forms of support. We will continue to strive to promote greater interoperability between our forces and those of partner nations; to further enhance information-sharing and consultations with nations contributing to NATO-led operations; and to offer partner countries NATO's advice on, and assistance with, the defense- and security-related aspects of reform.[4]

Because of the transnational nature of cyber defence, new global partnerships supported by the Alliance structure must play an essential role in extending NATO cyber defence capabilities. According to NATO officials, a large proportion of cyber attacks are launched from far outside the NATO theatre and thwarting or limiting these attacks necessitates close cooperation with non-Alliance countries. While NATO members may do much collectively to bolster their defences, the truth of the matter is that an effective strategy will require close working relationships with other nations and non-state actors. The NATO partnership process provides an institutional framework for such action to be taken. This framework should also be given the flexibility to develop closer relations with non-state actors such as corporations and non-profit groups which possess many of the tools needed to combat today's cyber threats. NATO already maintains a working relationship with alliance-based global information technology firms such as Microsoft, Google, and IBM as well as with international standards groups such as International Standards Organization (ISO) and the Internet Engineering Task Force (IETF). However, in order to make progress against cyber threats unleashed by non-state groups such as Al-Qaeda and Lashkar-e-Toiba in Asia, NATO members will need to develop closer ties to vital cyber actors in other regions in other parts of the world as well.

Another crucial area of global partnerships that will need to be addressed is one involving constabulary bodies such as Interpol. Since the majority of severe cyber attacks have a criminal component, NATO needs to develop close relations with police bodies. Each country has a different degree of cooperation when it comes to military and police relations, but the shared threat in global terrorism has already stimulated much innovation on this front. International security agencies can also benefit from a closer relationship with NATO and efforts should be made to ensure an effective exchange of real-time intelligence and forensic data. However, in order for this type of relationship to effectively detour cyber criminals, NATO officials must pave the way with clear policies and directives so agencies can feel empowered to share information among Allies without the threat of political recriminations at the local or national level.

4. The Digital Battlefield

While the bulk of NATO's cyber defence efforts will be aimed at defending civilian infrastructure from either state sponsored or non-state sponsored attack, NATO must redouble its efforts to secure its own forward deployed information systems from attack. The 21st century battlefield is rife with advanced information technology, making basic military operations increasingly vulnerable to devastating cyber attack. While few adversaries have demonstrated any real ability to severely disrupt NATO command and control systems via offensive cyber action, it can be surmised that future offensive strategies will call for a more overt use of cyber tactics on the digital battlefield.

There is much work to be done. A U.S. 'voice network systems journeyman' at Langley Air Force Base, Virginia
(Photo: U.S. Air Force Cyber Command/E.T. Sheler)

However, the growing interoperability gap between the U.S. and its European Allies presents a serious challenge to the Alliance's strategic objective of achieving total information dominance against adversaries on the digital battlefield. In order to anticipate and to defend against future threats, the NATO Consultation, Command and Control Agency (NC3A) in Brussels, and vital national command-and-control hubs will need greatly to increase efforts to keep current with the latest disruptive technology trends and innovations.[5]

Summary

Nearly two years ago, NATO member Estonia suffered a devastating cyber attack on its critical Internet infrastructure. While no souls were lost as a result of the attack, the severity and duration of the assault prompted a national crisis within the NATO alliance. The e-raid on Estonia also demonstrated the types of dynamic challenges the Alliance faces in a multipolar networked world. To its credit, the Alliance reacted quickly to the crisis and developed a provisional set of tools and capabilities to help its members to defend against future attacks.

While there is still much work to be done on this issue, NATO members should be reassured that the Alliance is indeed heading in the right direction. Cyber defence has also become an important building block and confidence building measure within NATO transformation. Since the scope and complexity of the issue will likely require the release of many trial balloons, NATO has already achieved two important milestones in the crafting of its 'Cyber Defence 1.0':

1) A real-time operational capability with the creation of the Cyber Defence Management Authority (CDMA);
2) An intellectual platform for long-term doctrinal and strategic thinking about the cyber domain through the formation of the Estonian-based Cooperative Cyber Defence Centre of Excellence (CCD CoE).

With these two instruments NATO started to show some teeth for combating real cyber threats. However, as the recent Russian aggression towards Georgia has shown, these teeth may not be sufficiently sharp to ward off any mischievous cyber bears or other e-adversaries seeking to compromise or destroy NATO digital assets deployed in either the Euro-Atlantic community or the 'near abroad'.

Dr. Rex B. Hughes is a co-founder and director of the Cyber Security Project at Chatham House in London and is a Research Associate of the Cambridge University-MIT Institute. His current research examines why the absence of a coherent global cyber security regime may threaten the structural integrity of the international trading order. Prior to his Cambridge years Hughes directed the world's first multidisciplinary Internet Studies program at the University of Washington where he led the development of 'iEnvoy', the first secure diplomat-to-diplomat Internet communications platform deployed by the U.S. Department of State.

Would you like to react? Mail the editor at info@atlcom.nl

1. The DOS attack on Estonia in short time followed the relocation of a highly-controversial Red Army soldier statue in Tallinn during the spring of 2007.
2. NATO Centers of Excellence are charged with facilitating transformation across NATO. CoEs are open for participation by all NATO member states, are nationally or multi-nationally managed and funded, and provide opportunities for NATO and Partnership for Peace nations to improve interoperability and capabilities, develop doctrine, and validate operational concepts through experimentation.
3. To date the only major international treaty on cyber crime is the European Council Convention on Cyber Crime. As of 2007 the Treaty included 43 European members and 15 other, non-European countries.
4. Section 31, Bucharest Summit Declaration (2008).
5. NC3A was formed in 1996 from the merging of the previous SHAPE Technical Centre (STC) in The Hague and the NATO Communications and Information Systems Agency (NACISA).

To learn more about cyber warfare and defence, have a look at the following online information:
- Kathryn Kerr, 'Putting Cyberterrorism into Context', Australian Computer Emergency Response Team, at: www.auscert.org.au/render.html?it=3552&template=1.
- Institute for the Advanced Study of Information Warfare: www.psycom.net/iwar.1.html, including a Glossary of Information Warfare Terms: www.psycom.net/iwar.2.html.

NATO
OTAN

Addendum

Atlantisch Perspectief no. 8, 2008 has been co-financed by the North Atlantic Treaty Organisation. Unfortunately this information and the NATO logo had not been included in that issue's colophon.