NIM/Cyber 14 September 2011

Talking Points

Subject: (S//REL NATO) NATO Civilian Intelligence Council—Cyber Panel National Input

A. Threat Overview (U)

(U//FOUO) Thank you for the opportunity to discuss our assessment on the cyber threat to NATO. I would like to start by making a clear distinction between the terms "cyber espionage" and "cyber attack":

- Cyber espionage is the theft of information that is being stored or transmitted as digital data.
-
- Cyber attack refers to malicious activity intended to disrupt data networks or deny access to them, to manipulate or corrupt the data on them, or to cause physical damage to infrastructure and equipment connected to them.

(S//REL NATO) We believe it is important to maintain a clear distinction between cyber espionage and cyber attacks because the probability of, consequences from and response to the two types of cyber incidents are distinctly different. The vast majority of cyber incidents against NATO networks are cyber espionage, not cyber attacks.

(S//REL NATO) We assess that cyber espionage is—and will remain—the principle threat to NATO systems over the next three years. We judge that cyber attacks against NATO networks by most nation states, including Russia and China, are unlikely outside of the context of a diplomatic or military conflict. However, we are concerned that the access that adversaries gain from cyber espionage activities could accelerate the deployment of cyber attacks in the event of such a conflict.

B. Specifics (U)

B1: Threat Actors (U)

(S//REL NATO) Russia poses the greatest cyber threat to NATO computer networks due to its strategic interests, its record of effective cyber collection, and its capability to target and disrupt NATO and member state computer infrastructures.

- (S//REL NATO) Russia is a robust, multi-disciplinary cyber actor with proven access and tradecraft which can conduct the full scope of operations, including computer network exploitation, insider-enabled operations, supply-chain operations, and computer network attack.

- (S//REL NATO) In addition, Russian nationalist hackers—who previously conducted cyber attacks against Estonian and Georgian networks—could target NATO systems in the event of a military or diplomatic conflict that pitted NATO against Russian interests.

(S//REL NATO) China lags behind Russia in terms of sophistication, but the scale and scope of their overall cyber activities and their increasing interest in information associated with NATO and its member states makes them the second most strategic threat to NATO networks.

- (S//REL NATO) Beijing has dramatically expanded its cyber espionage operations in the last five years and has conducted network intrusions—probably sponsored by the People's Liberation Army—against US military and diplomatic organizations.

- (S//REL NATO) We judge that China's concerns over NATO activities on its periphery, including ISAF operations in Afghanistan, almost certainly would make NATO information and networks a target for Chinese cyber espionage.

(S//REL NATO) Although "hacktivist" groups such as Anonymous have made headlines recently with their theft of NATO information, the threat posed by such activity is minimal relative to that of nation-states.

- (S//REL NATO) One area of concern, however, is the possibility of nation-states using hackers as proxies for their own operations. Difficulties with real-time attribution make it difficult to quickly identify threats, meaning that cyber espionage or cyber attacks can be disguised as cyber-crime or patriotic hacking activity. The example of Russian nationalist hackers targeting Estonia and Georgia serves to underscore this concern.

B2: Methods (U)

(S//REL NATO)

(S//REL NATO) We assess that any unclassified NATO network that is directly connected to the Internet should be considered potentially compromised, creating uncertainty regarding the confidentiality, integrity and continued availability of all data on that network. Spear phishing, although relatively unsophisticated at a technical level, has proved to be an effective intrusion method for many malicious actors. Full implementation of security best practices would help to significantly reduce the threat of cyber espionage against unclassified networks.

(S//REL NATO) As former deputy secretary of Defense William Lynn pointed out in a media article, in 2008 classified US military systems were infected with a cyber exploitation tool deployed by a foreign nation state, exemplifying the potential threat to protected military networks. We assess that the most immediate threat to classified NATO networks are insiders working on behalf of third-party nation states and unwitting NATO officers who create vulnerabilities by mishandling classified information systems and data, such as emailing classified NATO information through Internet-connected systems or using an infected thumb drive with classified computers. In addition, the presence of Russian intelligence officers operating in NATO spaces raises the risk of close access penetrations. Without the implementation of more robust security policies, monitoring tools, and training to counter these factors, we assess that any data on classified NATO networks is at potential risk.

B3: Other Factors (U)

(S//REL NATO) The discussion so far today on the threat actors and the methods they could employ represents the standard methodology for discussing and evaluating potential solutions to cyber security. A threat-based analytical model is useful for understanding the problem, but it only captures part of the picture.

(S//REL NATO) An alternative way to think about the defense of NATO's networks is to start by identifying which NATO data or networks would have the most consequences if they were stolen or disrupted, and work from there. Prioritizing the data and networks we need to protect the most would make it easier to map NATO gaps and vulnerabilities to actionable solutions, develop mitigation and response plans, and enable us to better allocate scarce resources.

(S//REL NATO) Separately, NATO’s efforts to work with non-Alliance members on cyber security issues are commendable. The Alliance’s ongoing work with the European Union and recent discussions on partnering with India only underscore the point that this is a global issue that affects everyone. We appreciate the Alliance’s efforts to improve its own cyber defenses and look forward to continued work in this area.

Prepared by: Jessica Vielhuber
NIC/CY – National Intelligence Council
[REDACTED] (secure)