The Holes in NATO's Cyber Defense Pledge

NATO Members Hack Each Other All the Time

By **Bill Blunden**, September 4, 2014

NATO members are currently meeting in Wales to consider a joint defense agreement which stipulates that a cyberattack on one member would represent an attack on all of them [1]. Though the concept of international teamwork may seem appealing at the outset there are at least a couple of issues that officials are [intentionally] neglecting.

High-End Anti-Forensics

For instance, how can countries mobilize to fend off a cyberattack when they can't even tell who launched it? Deception is an age-old instrument of spy tradecraft and the Pentagon has been actively working on developing Internet stealth technology for decades.

The Tor platform, for example, is based on a technology called *onion-routing* which sends encrypted network traffic through a cloud of relay computers in an attempt to conceal the source of the traffic. Former military researcher Michael Reed admits that onion routing was originally invented years back on behalf of spies [2]:

> *"The *PURPOSE* was for DoD / Intelligence usage (open source intelligence gathering, covering of forward deployed assets, whatever). Not helping dissidents in repressive countries."*

Though it receives funding from the military [3], Tor is a poor man's anonymity suite. As such it's fallible and has been successfully undermined by U.S. security services on a number of occasions [4]. Contrary to popular belief the people caught weren't always incompetent. Some of them were technically proficient [5].

Professional spies (you know, the guys with an $80 billion budget) tend to use their own custom platforms. Classified documents reveal that spies regularly scan the internet for vulnerable computers, subvert them with malware, and then merge the compromised machines into a globe-spanning command and control infrastructure. That's right, the intelligence outfits are creating their own anonymity botnets [6].

> *"Several times a year, the spy club tries to take control of as many machines as possible, as long as they are abroad. For example, on February 2010 twenty-fourth spies located over 3000 potential ORBs in a single work day"*

Funny, this is exactly the same technique used by criminals [7]. How about that?

Seeing an opportunity to make a buck, the private sector has also jumped on this train. Thanks to WikiLeaks we know about a company named Ntrepid that offers an anonymity service called the Internet Operations Network (ION). The company's glossy marketing literature states [8]:

> *"ION solutions are built on proprietary technologies that provide multiple layers of indirection, ensuring no link exists between mission personnel and their assets, or between assets. With technologies that transcend simple non-attribution, our hardened security leaves no trace of operational communication."*

Black Hats Turn to Old Hat

The hi-tech tools utilized by government spies and purveyed by companies like Ntrepid are augmented by traditional covert measures. You know, the kind of old school stuff you'd read about in a John le Carré novel. Groups like the NSA's Office of Tailored Access Operations (TAO) leverage front organizations, fake identities, and limited hangouts [9]:

> *"TAO increasingly depends on clandestine techniques, such as commercial cover, to hide its activities. TAO uses an array of commercial business entities, some of them proprietary companies established specifically for this purpose, to try to hide its global computer-hacking activities from computer security experts in a maze of interlocking computer servers and command-and-control systems located in the United States and overseas that have no discernible link to the NSA or the U.S. government."*

How can you possibly track down an attack when the ISP hosting the attack is itself a shadow organization?

What all this means is that just because network traffic is coming from a particular country (ahem, China or Russia) doesn't mean that Chinese or Russian hackers are to blame. Attacks could be the result of a false flag operation. Documents published by the *Intercept* corroborate this. They describe a whole series of dirty tricks used by GCHQ's Joint Threat Research Intelligence Group (JTRIG). One of the techniques in JTRIG's operational playbook is, a drumroll please …false flag operations [10].

Cyber Lord of the Flies

There's another catch to the NATO's joint defense scheme. A joint defense agreement is founded on the notion of an external enemy. Can such a pledge withstand the pressure of substantial internal threats?

A house divided against itself cannot stand: the United States Hacks Germany [11], Germany Hacks the United States [12], Germany Hacks Turkey [13], The Israelis hack the United States and the United States hack Israel [14]… I think you get the picture. The idea that NATO members would rally around a common defensive perimeter is laughable because report after report reveals the inconvenient truth that NATO members are too busy breaking into each other's networks.

Folks, it's anarchy. Until we mobilize and get our political leaders to outlaw covert ops the government and corporate spies show no sign of letting up. In all probability, as things progress the whole clandestine scene is just going to get worse. This past April Obama openly bragged to China's leadership that the U.S would be devoting $26 billion to the Pentagon's cyber trough and expanding the U.S. force to 6,000 so-called "cyberwarriors" [15]. Guess where all of that funding goes to?

The moral of the story is this: when high-level Pentagon types and think tank pundits start yammering about cyberattacks from Russia or China keep in mind that our security services are neck deep in deception ops directed against their alleged allies. History shows that the American Deep State is constantly in search of new enemies, even if it has to fabricate them[16], and our corporate rulers have no scruples about launching attacks that kill untold thousands of innocent people so that they can boost quarterly profits.

Bill Blunden is an independent investigator whose current areas of inquiry include information security, anti-forensics, and institutional analysis. He is the author of several books, including *The Rootkit Arsenal* and *Behold a Pale Farce: Cyberwar, Threat Inflation, and the Malware-Industrial Complex*. Bill is the lead investigator at Below Gotham Labs.

End Notes

[1] David Sanger, "NATO Set to Ratify Pledge on Joint Defense in Case of Major Cyberattack," *New York Times*, August 31, 2014.

[2] "TOR Made for USG Open Source Spying Says Maker," *Cryptome*, March 22, 2011.

[3] Yasha Levine, "Almost everyone involved in developing Tor was (or is) funded by the US government," *Pando*, July 16, 2014.

[4] Bill Blunden, "The NSA Wants You to Trust Tor, Should You?," *Counterpunch*, July 18-20, 2014.

[5] Kim Zetter, "Federal Cybersecurity Director Found Guilty on Child Porn Charges," *Wired*, August 26, 2014.

[6] Julian Kirsch, Christian Grothoff, Monika Ermert, Jacob Appelbaum, Laura Poitras, Henrik Moltke, "NSA/GCHQ: The HACIENDA Program for Internet Colonization," *Heise Online*, August 15, 2014.

[7] Sergey Golovanov and Igor Soumenkov, "TDL4 – Top Bot", *SecureList*, June 27, 2011.

[8] https://www.wikileaks.org/spyfiles/docs/NTREPID-2011-IONInteOper-en.pdf

[9] Matthew Aid, “The NSA’s New Code Breakers,” *Foreign Policy*, October 15, 2013.

[10] Glenn Greenwald, “How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations,” *Intercept*, February 24, 2014.

[11] “Embassy Espionage: The NSA's Secret Spy Hub in Berlin,” *Der Spiegel*, October 27, 2013.

[12] Alexandra Hudson, “German security recorded Clinton conversation: media,” *Reuters*, August 15, 2014.

[13] “Targeting Turkey: How Germany Spies on Its Friends,” *Der Spiegel*, August 18, 2014.

[14] Glenn Greenwald, Laura Poitras and Ewen MacAskill, “NSA shares raw intelligence including Americans’ data with Israel,” *Guardian*, September 11, 2013.

[15] David Sanger, “U.S. Tries Candor to Assure China on Cyberattacks,” *New York Times*, April 6, 2014.

[16] Bill Blunden, “The Zero-Sum Game of Perpetual Conflict,” *Counterpunch*, September 2, 2014.