OLD WINE IN NEW BOTTLES: NATO AND CYBERSECURITY

Daniel Little
(RIEAS Senior Advisor)

The old biblical adage of not putting 'old wine into new bottles' has been used countless times in a variety of disciplines. In this example, NATO could be construed as being that 'old wine' yet this generalization does not have to be so. When confronted with paradigm shifts, NATO did adopt itself to the surrounding circumstances it faced. The starkest examples were its performance in Kosovo as the backbone of KFOR, the Declaration of Article V during 9-11 and later its deployment as ISAF in Afghanistan.

Unfortunately, the parallel to 'old wine' is where artificial and unrealistic barriers hamper NATO's ability to protect its citizens. One such barrier to consider is the EU's initiatives to protect privacy data.[1] To be fair, citizens of the EU deserve to have their civil liberties and privacy protected just like everywhere else. However laudable, there are unintended consequences if cybersecurity is prevented from doing the same thing.

The examples are numerous but I will only highlight a few. Recently (May 22, 2013), the murder of a British soldier by Muslim extremists prompted far-right protestors to take to the streets. In retribution, a hacker published the names and addresses of 270 Far-Right supporters belonging to the English Defence League (EDL).[2] Presuming that the attackers were influenced outside Britain, why is a violation of personal data treated as domestic when external factors

and influences are possibly causal to both the incident that occurred as well as the response that followed?

On a grander scale, what if a cyberattack moves through one NATO country to attack another? Presuming that the target is the U.S., the response would be for the relatively new U.S. Cyber Command (USCYBERCOM)[3] to engage in cyberwarfare. The problem with that approach is that U.S. contractors supporting USCYBERCOM risk fines of 2% of worldwide gross income for targeting those within the EU.[4] With such potential for contentiousness, transatlantic division only serves the interests of those hostile to NATO.

Looking back, the first acknowledged attack was in 1999 during OPERATION ALLIED FORCE; an air campaign seeking the expulsion of Serb military forces out of Kosovo. In response, hackers undertook the defacement and denial of service (DDOS) of NATO's website. By 2007, the scope of DDOS was such that Estonia's governmental, political, banking and news agencies were shut down. Although there were incidents during the 2011 OPERATION UNIFIED PROTECTOR in Libya, the effects were more tantamount to harassment than attack.[5]

As early as 2008, Suleyman Anil amongst others warned what implications awaited cybersecurity. Although the targeting of cyberattacks were directed towards communication networks and official institutions,[6] he accurately addressed the target but could only allude to the means. With Moore's Law lowering the barrier of entry, the potential payoff made a secluded room of computers all the more lethal a weapon as bomber aircraft with twice the stealth.

The key difference between the old bottle and new one is the intended target. In the old paradigm, cyber activities were undertaken to prove it could be done. In the new bottle, the stakes are much higher. Let there be no mistake, Cybersecurity involves information and information is power. Whether political, economic or military, information is as much rooted in national power and interests as it was in Sun Tzu's time. Here are a few recent examples. A short-lived hoax on Twitter reported explosions at the White House. Although the hacking and ensuing denial was equally quick, $200 billion of market value were erased from Wall Street. Why? There were algorithms scanning news feeds.

The sell orders were generated automatically as a way for select traders to stay one step ahead of the competition.[7] In other words the mere coupling of words affected people's livelihoods, reputations and pensions. Late last year Former U.S. Secretary of Defense Panetta released that the hacking of chemical, electricity and water plants were successful which if implemented could create panic and potential loss of life. Panetta also confirmed that a recent virus attack disabled 30,000 computers belonging to the Saudi oil company Aramco.[8]

Consider then the following questions. Is there a consensus similar to Article V – 'where an attack upon one is an attack upon all,' regardless of where it originates and how? If NATO member countries do not truly believe they are at war, what defines winning as the ultimate

objective? If NATO's Cyber Defence Management Authority (CDMA) and Cooperative Cyber Defense (CCD) Center of Excellence are not given the means and license to attack, even counterattack, how can Clausewitz' defined goal of 'defeating the enemy's will to fight be realized?' If not what good is early warning and 'Smart Defense' initiatives[9] if the livelihood and well-being of everyday citizens fall victim to a 'Cyber 9-11.'

Herein lies the greatest of contradictions. The field of cyberbattle is behind a screen not a remote province. The treasure of a nation's competitive advantage is not the gold in its bank vaults but the intellectual property and critical infrastructure embedded in its servers. Worst still is that the most affluent of countries arbitrarily choose not to defend their smaller neighbors much less themselves by taking offense off the table. Originating from the Maginot and Siegfried Lines, NATO was ushered in alongside Mutually Assured Destruction (MAD) and *Realpolitik*.

Instead of missiles, 'white-hat,' ethical hacking tests reverse proxy security configurations, while Information Assurance 'battle drills' can be pre-coordinated, pre-approved and tested so that restoration can occur to thwart further penetrations. But is that enough? In regards to retaliation, NATO became what it was because of what bound it together not its clear differences. The prospect of 28 member countries working together is supposed to serve that deterrence. While testing the alliance is a given, it is the strength of that response that ultimately determines what happens afterwards. Unless it is made absolutely clear, the prospect of old wine being placed in a new bottle will only serve as further encouragement.

Notes:

[1] European Commission (2012). "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," January 25, 2012 [Available for Download] http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Accessed May 29, 2013]

[2] RTonline (2013). "#AnonymousUK Hackers post far-right members' contact details online." TV-Novosti [online], http://rt.com/news/edl-hackers-contact-details-932/ [Accessed May 29, 2013]

[3] Harris, G. (2010). "The Pentagon's New Cyber Command" ISN: ETH Zurich, [Available for Download] http://www.isn.ethz.ch/isn/Digital-Library/Articles/Detail/?id=125766&lng=en [Accessed May 29, 2013]

[4] MLaw Group (2012). **"**New draft European data protection regime to apply also to all US companies processing data of European residents**."** MLaw Group [online], Feb 2, 2012 http://www.mlawgroup.de/news/publications/detail.php?we_objectID=227 [Accessed May 29, 2013].

[5] Healey, J. and van Bochoven, L. (2012). "NATO's Cyber Capabilities: Yesterday, Today and Tomorrow." [Available for Download] http://www.acus.org/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf [Accessed May 30, 2013]

[6] Johnson, Bobbie (2008). "NATO says Cyberwarfare poses as great a threat as a missile attack." The Guardian, March 6, 2008, [Available for Download] http://online.wsj.com/article/SB10001424127887323735604578441201605193488.html [Accessed May 29, 2013]

[7] Lauricella, Tom, Stewart, Christopher and Ovide, Shira (2013). "Twitter Hoax Sparks Swift Stock Swoon." The Wall Street Journal, April 23, 2013, [Available for Download] http://online.wsj.com/article/SB10001424127887323735604578441201605193488.html [Accessed May 29, 2013].

[8] Hoover, J.N. (2012). "DoD: Hackers Breached U.S. Critical Infrastructure Control Systems." Information Week Government, October 12, 2012, [Available for Download] http://www.informationweek.com/government/security/dod-hackers-breached-us-critical-infrast/240008972 [Accessed May 29, 2013]

[9] Healey, J. and van Bochoven, L. (2012). "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO." Atlantic Council, November 6, 2012, [Available for Download] http://www.acus.org/publication/strategic-cyber-early-warning-phased-adaptive-approach-nato [Accessed May 29, 2013]

[10] Hughes, R. (2009). "NATO and Cyber Defence: Mission Accomplished?" Atlantisch Perspectief, 1/4 [Available for download] www.atlcom.nl/site/english/nieuws/wp-content/**Hughes**.pdf