Journal of Defense Management
ISSN: 2167-0374

Acharya and Acharya, J Def Manag 2017, 7:1
DOI: 10.4172/2167-0374.1000159

Opinion Article Open Access

Internet of Things, Ransomware and Terrorism

Arabinda Acharya[1]*and Amrit P Acharya[2]

[1]Department of International Security Studies, National Defense University, Fort Lesley J. McNair, USA
[2]Associate McKinsey & Company, USA

Abstract

The new form of ransomware attack going by the name "WannaCry" (Ransom.Wannacry) demonstrated how vulnerabilities in the cyber domain can be used to cause mass-scale chaos and shutdown of services and utilities including hospitals, transportation networks and others even though for a limited period.

Keywords: WannaCry; Cyberspace; Terrorists; DNA Sequencing Data; Bioterrorist; Mass Disruption

Introduction

Hundreds of thousands of computers in more than 150 countries across the world were affected and hundred thousand dollars were paid by victims as ransom before a cyber-activist in the UK shut down the spread. The threat however is not over as experts believe that perpetrators and copy-cat hackers can develop mutants of the virus and cause the mayhem again.

Is it then possible that terrorists would be interested to use similar tactics? This may sound alarmist especially due to the limited and reversibility nature of the impact of the WannaCry attack and terrorists' conventional aversion to use the cyberspace to deliver attacks. However, it is difficult to brush off the threat in a wider context if we consider the motivations behind and dynamics of terrorist attacks and the potential of attacks using cyber tools like WannaCry.

Terrorists' use of Cyber-space- Benign vs. Offensive

Traditionally, terrorists–irrespective of ideological or religious disposition-have used the cyber space for a variety of purposes most of which have been from a utilitarian perspective. These include propaganda and publicity, recruitment and funding and importantly networking among geographically dispersed community. More offensive uses of the cyberspace include data mining, mobilization and provocation for attacks (as against actual attacks), information sharing–tactics, technology, tradecraft and targeting for DIY attacks. Information disseminated in the cyber space also includes use of chemical and biological weapons and delivery options and importantly, justification of the same in the name of the religion. The most direct form of cyberterrorism has been Denial Of Service (DoS) attacks and website defacements.

However, this could change with increasing technical competency and capability for network-based attacks and growing number of hackers in the online community. Opportunity for online interaction and training has compensated terrorists the loss of physical space for such activities on the ground. New generation social networking tools such as Facebook, Twitter, Orkut and Second Life, Telegram, among others, provide platforms not only to share information and expertise but also practice it in virtual space. Second Life in fact is populated with a number of virtual terrorist groups -"Elite Jihad Terrorist Group," "Jihad Terrorists," "Second Life Qaeda," "Second Life Terrorist Association." In 2007, Second Life Liberation Army (SLLA) set off virtual bombs at virtual stores and buildings. Virtual terrorists also attacked the offices of ABC News, American Apparel and Reebok. Even as these activities appear to be video-game reproductions, their real-life implications cannot be underestimated.

What Changed with Ransomware?

Hacking tools like WannaCry have the potential to reduce the opportunity cost for terrorist attacks. For example, even though groups like Al Qaeda and the Islamic State of Iraq and Syria (ISIS) have demonstrated interest in and some capability to develop and use chemical, biological, radiological, or nuclear weapons (CBRN), there has been no successful mass casualty terrorist attacks involving them. This is attributed to terrorists' inability to weaponize these materials. Moreover, there is the concern that perpetrators might lose control over the consequences of such an attack that could affect the members of the communities they are purportedly fighting for. However, use of weapons of "mass disruption" like ransomware as against weapons of "mass destruction" will enable terrorists to cause large-scale damage (loss of data and equipment), chaos (in hospitals and other public utilities) and fear. Imagine the impact if terrorist groups like Al Qaeda or ISIS were involved in WannaCry attack. For terrorists, it's a win-win tactic as they can achieve almost similar attention and without firing a shot or exploding a bomb. Additionally, terrorists may even be able to get away with some money to fund their future activities.

These tools are especially attractive due to vulnerabilities in certain industries and services, targeting of which can have strategic level impact. These sectors continue to use aging infrastructure. According to a report of the US Bureau of Economic Analysis, in the US, the average age of all fixed assets stood at 22.8 years in 2015, the oldest in records going back to 1925. Hospitals and utilities are some of the worst culprits. A 2015 study by McKinsey and Co., which ranked US industries by most digitized to least digitized, placed construction, hospitality, healthcare, government and agriculture at the bottom of a digitization index in that order. While this may not always be an issue in public safety, it does pose some risks as new technology vendors have to integrate with and be interoperable with sometimes decades old legacy technologies which were built in a world without the internet and where cyber terrorism did not exist. In fact, hospitals and public services were some of the worst affected by WannaCry where entire hospitals were shut down as also some public services such as transportation (railway) systems in Russia, India, Europe and others across the world.

***Corresponding author:** Arabinda Acharya, Department of International Security Studies, National Defense University, USA, Tel: +1 202-685-4700; E-mail: arabindaacharya@gmail.com

Received May 29, 2017; **Accepted** June 26, 2017; **Published** June 29, 2017

Citation: Acharya A, Acharya AP (2017) Internet of Things, Ransomware and Terrorism. J Def Manag 7: 159. doi:10.4172/2167-0374.1000159

Thinking of the Worst

Despite being at the bottom of the digitalization index, agriculture is becoming "smarter" every day with more and more farmers relying on data driven decision making, either through sensors planted on the ground or satellites guiding tractor movements and decisions on agronomic practices from above. A report by Business Insider Intelligence estimates that the by 2030 average US farm sector is likely to generate 2 m data points per day-up from just 200 k now. Global technology companies such as IBM, Cisco and GE are already gearing up for this new market, with investments into the so-called "Internet of Things" likely to grow by 16% every year to $250B by 2021 with agriculture as one of the top opportunity markets.

While this has exciting implications on the potential to dramatically improve farm yields (some studies have shown improvements by as much as 30%), according a report by the US Federal Bureau of Investigation (FBI) increased adoption of "precision farming" technology exposes the agriculture sector to the risk of hacking and data theft similar to WannaCry ransomware.

Network-based integration of modern tools, mostly provided by third-party vendors, with legacy pre-Internet age technologies however creates vulnerabilities especially in terms of data theft. For example, Monsanto's FieldView platform which provides a mesh network to integrate all farm sensors (both new and legacy) to create an "Internet of farms," is also building a single point of failure which if hacked would compromise the entire system. In fact, in 2014 a "Digital Agriculture" startup acquired by Monsanto was hacked compromising credit card and employee information. As Robert Fraley, Monsanto's chief technology officer explained, "As an industry, we're still new to it (hacking)."

Another emerging but related vulnerability in the bio-technology sector is gene editing tools such as CRISPR-CAS9 (Clustered Regularly Interspaced Short Palindromic Repeats). CRISPR helps scientists to precisely alter, delete and rearrange the DNA of every major living organism quickly. The aim is to curing diseases in humans or in the case of agriculture, developing the next generation of genetically modified organisms to improve crop yields.

However, as Michael Specter describes "there has never been a more powerful biological tool or one with greater potential for benefit and harm." CRISPR, not only democratizes the potential for intentional misuse by anyone with access to the underlying DNA sequencing data and a computer with the necessary software, but also makes it extremely inexpensive to do so. DNA sequencing no longer requires sophisticated labs, years of experience or huge amount of money. Simple Do-It-Yourself CRISPR kits are available commercially on the Internet for less than $150. These advances in genome sequencing allow scientists to quickly and cheaply generate the DNA sequence of entire organisms, and also easily digitize it and store it for research use–information that could be used by terrorists to design bioweapons and hold governments to ransom.

All that a determined bioterrorist needs to do is just walk into an unmonitored farm land or into the corporate field labs of big agriculture companies, steal seeds, and then reverse engineer it into a bioweapon with software based gene editing tools like CRISPR. They can create modified pests with the ability to destroy entire farm land –a possibility that British entomologist Jeffrey Lockwood highlighted in his book "Six-Legged Soldiers: Using Insects as Weapons of War." Terrorists can also introduce new breeds of corn, for example, which reproduces faster than local breeds, but is not safe for human and/or animal consumption. These are not entirely unlikely as evident from increasing level of attacks on the global food chain by animal rights and environmental extremists.

New-age technologies are a boon or a bane depending on whose hands they are in. Increasing levels of computer literacy, Internet and social networking tools create immense opportunities for higher innovations across all sectors. But these are also creating vulnerabilities which hackers exploit. So far this has remained in the realm of hackers with criminal intent but there is no reason to assume that terrorists will not exploit these vulnerabilities in one way or the other in future.

Conclusion

Though technology adoption in diverse sectors is happening in a very fast pace, measures to secure data are lagging behind or even lacking. This has exposed these sectors to software viruses and ransomware attacks such as WannaCry. Unfortunately, this has missed serious attention by concerned agencies including governments so far. This could be due to lack of ownership of the problem as reinforced by repeated data breach involving government and the private sector.

Is it likely to change if a data breach is attributed to a terrorist group? Groups like Al Qaeda and ISIS have repeatedly demonstrated their ability to use media–old and new. In many cases, some groups appear to be ahead of governments in the learning curve as our response has been and continues to be reactive. From another perspective, terrorists need not carry out an actual operation–even an attempt is sufficient to impact normal life as was with the "liquid plot" and now with the ban on carrying laptops while travelling. Given the fact that terrorists' may not so much be interested in body counts as the impact of their actions to cause fear, chaos and inconvenience, hacking tools like WannaCry ransomware could be as potent as suicide bombings.

Trends in new-age terrorism have demonstrated how governments are often caught unaware by attacks that use the most seemingly innocent and unlikely tools. Is it therefore the time to wake up to these new threats as it would be dangerous to under-react or worse, not to know how to react at all?