Understanding nation-state attacks

Eric Lundbohm, Veracity Industrial Networks

Eric Lundbohm

For the past three years the world has been going through an unprecedented increase in malicious cyber activity. Ransomware has mined a source of money that didn't exist just a few years ago. The emergence of nation states using cyber-attacks and breaches to further their agendas has caused an explosion of new threats against which every network must now have defences that work.

Indeed, security company Symantec, in its '2017 Internet Security Threat Report' (ISTR) concluded: "The world of cyber-espionage experienced a notable shift towards more overt activity, designed to destabilise and disrupt targeted organisations and countries."[1] This is a fundamental change in the goal and tenor of cyber activities. It is much more than cyber-attacks just for money.

Today's world has proved capable of producing staggering disasters at any time. The recent past has supplied us with myriad weather-related challenges, but from each iteration, we learn more and are better prepared for the next one.

"While there are nine nuclear countries, US intelligence officials reported in January 2017 that more than 30 countries are developing offensive cyber-attack capabilities"

That hasn't happened with a 'cyber 9/11'. We're still very early in our understanding of what havoc could be forced upon us due to a cyber-attack propagated by a nation state. Clearly there are nation states that have the capability to launch an offensive cyber-attack against another nation. While there are nine nuclear countries, US intelligence officials reported in January 2017 that more than 30 countries are developing offensive cyber-attack capabilities.[2]

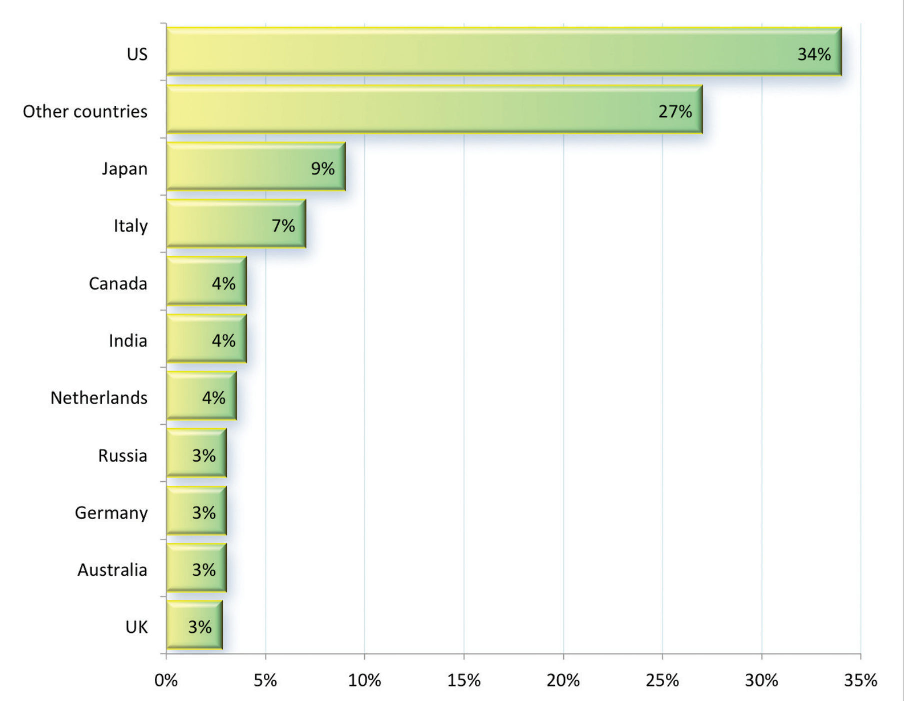
It's likely, therefore, that a sophisticated and co-ordinated cyber-attack that includes significant assaults on our communications, financial services and infrastructure is overdue. Also, for reasons detailed here, we may be at significant risk for an attack on our critical infrastructure in the next couple of years.

Up to date

Cyber warfare is more common than we think. So let's start by bringing everyone up to date. The US is fighting cyberwar on a daily basis. Since the original 'dot-com boom' and the subsequent wiring of the planet, having evil people do harm to others online has been part of the norm. Consequently, every military action we undertake has a cyber component to it. We spend large amounts of money on it too. The fiscal 2017 US Department of Defense (DOD) budget calls for spending $6.7bn for cyber operations, an increase of about $900m over fiscal 2016.[3]

This trend is likely to continue and cyber-attacks will ultimately be used as an offensive weapon. Why? There are many reasons that developing an offensive cyber capability is very likely a high priority for all the enemies of the US.

War is expensive. The US maintains the largest defence budget on the planet, which dwarfs all other nations' spending to a staggering degree. The US outspends China (the owner of the second largest defence budget) by a factor of almost three to one and outspends Russia by nearly nine to one.[4] It's sensible to assume that these nations are looking for ways to maximise their



Ransomware detections by region, 2016. Source: Symantec ISTR.

military power at a reasonable cost and cyber activities may be the answer.

Just a single traditional military operation can run to hundreds of millions of dollars. For example, the US attack on the Syrian airport in April 2017 used 59 Tomahawk missiles at a cost of $1.4m each.[5] That's $82m in 'ammunition' for that two-hour attack. And the costs do not end there. These missiles were launched from two 500-foot, $1.8bn Arleigh Burke-class guided-missile destroyers, each supported by almost 300 personnel.

David and Goliath

It's daunting for other nations to think about competing with that type of raw military power. However, it's likely that military strategists around the globe have recognised the opportunity to gain some parity with, or even some advantage over, the US by developing expertise in cyber warfare. There is a 'David and Goliath' quality to hacking, as single hackers have been successful in bringing down companies and networks. You can employ a lot of engineers for $82m and likely make good inroads on a cyber strategy.

"It's likely that the security of the power grid will be tighter in three years than it is today. A foreign actor could look at this and see a limited time span to compromise parts of the US power grid, prompting an attack based on opportunity"

Cyber-security for critical infrastructure may be at a low point. The US is in the midst of understanding and managing the cyberthreats to power, water and energy delivery systems. Technologies in development by cyber-security start-ups are figuring it out and so is the Government. Any public attack would hasten the development and adoption of new security measures. Due to these actions, it's likely that the security of the power grid, for example, will be tighter in three years than it is today. A foreign actor could look at this and see a limited time span to compromise parts of the US power grid, prompting an attack based on opportunity.

You only get one shot. Many point to the lack of a cyber 9/11 or really any major attack on the US power grid as evidence that it is unlikely to happen in the future. Nothing could be further from the truth. It's likely that a foreign actor would have but one real chance to disrupt the power grid on a large scale. Also, from what we know about how IT security has evolved, it's likely that intruders are in the systems, looking around, sometimes for long periods of time. IT security people talk about 'dwell time', which is the period between when an intruder first enters your system and when it is discovered. This number is in the hundreds of days at enterprise-size networks.

Many experts consider the recent cyber-attacks on the power grid in Ukraine to have been a form of practice in preparation for a more targeted attack on a larger enemy. Disk-wiping KillDisk trojan malware was used against targets in Ukraine in January 2016 and again in December the same year – attacks that also resulted in power outages, likely perpetrated by Russian cyber efforts.

Bang for buck

Many of the enemies of the US are intent on spreading terror. Terror is a bit of a mindset. Imagine the 'terror' that a national black-out would cause. Imagine the terror multiplying as a national blackout continued for days, weeks or months. Lastly, imagine all of this happening during a military action or a physical terror attack on US soil, such as a nuclear 'dirty bomb'. Terrorists often employ co-ordinated attacks to maximise effect. Cyber-attacks will be used in this manner in the future.

No-one actually gets hurt. One of the stark realities of traditional warfare is that people die. Military leaders estimate the body count of various actions. These are not concerns in the cyberworld. Sending your best and brightest off to invade via cyberspace with no danger to their physical well-being can make this type of warfare very attractive.

There's also a plausible deniability to cyber activities. With today's heavily satellite-surveyed world, we see ground evidence of most military activity very quickly. Submarines still pose a challenge, but things that are visible from the sky are visible to everyone now. This makes it hard to hide the movement of troops and equipment. Missiles are tracked by radar with certainty. However, cyber activity can be shrouded, spoofed, routed and made hard to track and identify its source. This muddies the warfare waters considerably. If you're not sure exactly who your enemy is, war will be imprecise at best.

Types of attacks

Cyber aggression sponsored by nation states is different from normal cybercrime. From the limited number of verified state-sponsored cyber activities, both the intent and the targets are large.

North Korea likely views cyber as a cost-effective, asymmetric, deniable tool that it can employ with little risk from reprisal attacks, in part because its networks are largely separated from the Internet and any disruption of Internet access would have minimal impact on its economy.[6]

When a nation state initiates offensive cyber-activity, in general the goals are large and usually aimed directly at another state entity. As mentioned earlier, nation states are much more apt to focus on disruption of basic services or communications than to be gathering items to be sold on the dark web. When nation states do go after money, it will likely be of the scale of North Korea's recent $81m cyber heist at the Bangladesh central bank.

North Korea in particular is known to have an active botnet in place capable of executing distributed denial of service (DDoS) attacks. This past May, an alert was issued by the US Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). This alert provides technical details on the tools and infrastructure being used by cyber actors in the North Korean Government to target the media, aerospace, financial and critical infrastructure sectors in the US and globally.[7]

Some researchers have also linked North Korea to the WannaCry ransomware attack, an outbreak of malware in May reported to have infected more than 300,000 computers in over 150 countries, making data irretrievable in many cases.[8] In December 2014, the South Korean Government reported that power plants operated by Korea Hydro and Nuclear Power were targeted with wiper malware, potentially linked to North Korean actors.[9]

In the future we should expect to see all of these forms of attack, particularly from North Korea. It is also likely that future attacks will be co-ordinated, for example, executing a DDoS attack on specific websites during a power grid action. It's also likely that cyber-attacks that impact critical infrastructure will be timed for maximum damage – eg, launching an attack on the US power grid during a blizzard or extreme cold conditions.

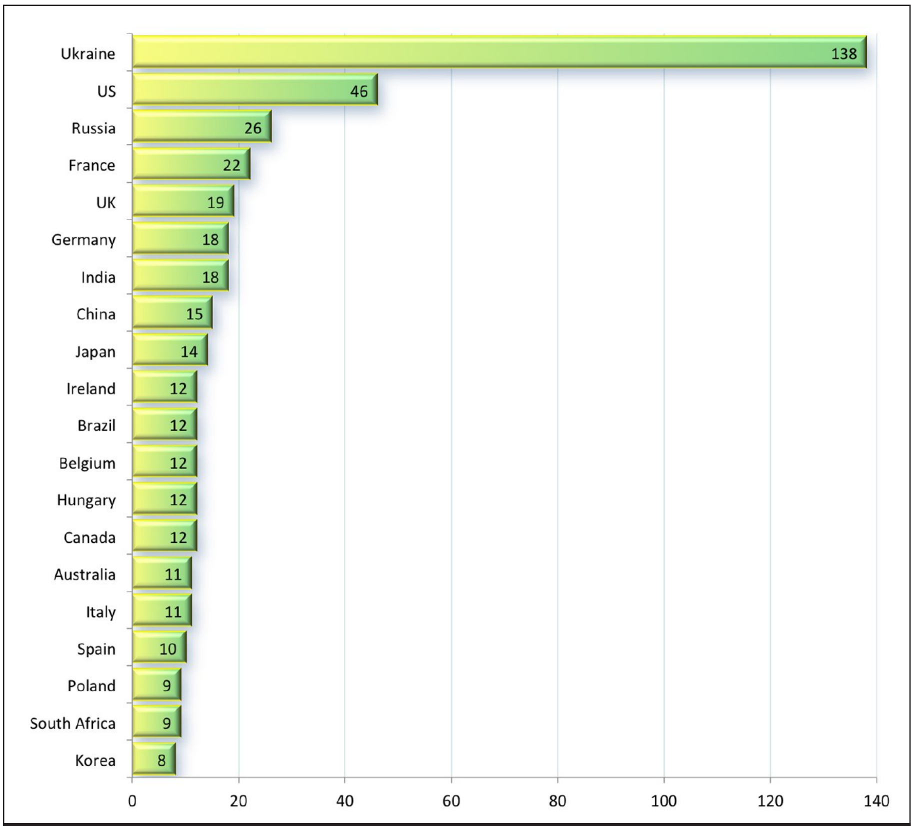
How do we respond?

Plainly, we need to focus attention on this issue and understand both the risk and consequences of potential cyber actions by nation-state actors. The risk and subsequent mitigation of risk is different than in the physical world.

Certainly the most attractive way of handling all this would be to implement cyber defences capable of protecting key assets from outside interference. This is the goal of most cyber-security efforts. However, we all know that sometimes even the best cyber defences are vulnerable and bad actors will penetrate these defences.

One of the standard US responses to offensive attacks of any kind is retaliation. Using the considerable cyber capabilities of the US to bring even greater havoc to an aggressor would be viewed as an appropriate and reciprocal response. However, all is not created equal. For example, while North Korea holds considerable offensive cyber capabilities, there is little to no infrastructure to attack. The country has almost no Internet and a primitive power grid to the point that there is nothing to target.

Lastly, having considerable cyber firepower may act as a deterrent to some nation states. For example, it could be that there is an unspoken doctrine of 'mutually assured destruction' between the leading cyber powers, not unlike the nuclear detente between the US and Russia. Either party knows it can do considerable harm via an offensive cyber-attack, but also knows that a catastrophic attack will likely be met by a similarly destructive counter attack.



Ransomware infections by NotPetya (also dubbed Petya by some organisations) as of 27 Jun 2017. This attack clearly targeted Ukraine. Source: Symantec ISTR.

Where does this all end?

It's hard to know where cyberwar ends up. There is already a defensive posture in place. It's also possible the US will use cyber weapons offensively on another nation state. Now, once again, we may not see airplanes with US markings do the bidding of the US (See "Stuxnet) but learn of our international victories much after the fact without confirmation by any government. Such is the theatre of cyberwar.

Clearly, we also aren't going to see the progress that enemies make in the cyber arena in the same way we can see North Korea's Kim Jong Un's progressive ballistic missile tests. It's unlikely that those nation states that have the cyber equivalent of North Korea's missiles will advertise that fact and demonstrate the progress for the world to see. Cyber-attacks essentially exploit weaknesses in the system and cyber-defences plug those vulnerabilities, making a surprise attack all the more powerful.

We shouldn't draw massive conclusions about cyber warfare norms by observing North Korea. There have been some attacks from North Korea that have affected some specific large corporations. The Sony movie hack in 2014 was just that – an outreach from a nation state on the assets of a publicly held corporation. While retaliating for an insult in a movie is unlikely to be a normal part of international cyber diplomacy, military suppliers and contractors are often targets.

Bottom line

The US lost its terrorism virginity during the 9/11 attacks. Terrorists changed the course of history with one morning's activity. Unfortunately, there's a chance we'll see history repeat itself with a debilitating attack on the US critical infrastructure networks that control the critical water, power and transportation infrastructure.

What might be different with this attack is the personalisation that comes from direct involvement with the disaster. An attack that compromises power or water systems can affect every person at a very basic level and hence will be taken very personally. These may also be attacks that will not be over or forgotten so quickly.

In any of these events, we live in a world where battles are and will increasingly be fought in cyberspace rather than on the ground and in the air. While this is a cleaner style of war, without the physical devastation of bullets and bombs, it is no less a threat.

About the author

Eric Lundbohm has three decades of marketing and executive experience, including over 15 years of cyber-security industry background. He currently serves as chief marketing officer of Veracity Industrial Networks (www.veracity.io), a developer of Industrial SDN-based technology for operational networks. Lundbohm's background in cyber-security has been shaped by running marketing for several security firms, including M86 Security, iSheriff and NSS Labs. He holds a master's in business administration from Ohio State University and a bachelors in management information systems from the University of Rhode Island.

References

1. '2017 Internet Security Threat Report (ISTR)'. Symantec. Accessed Oct 2017. https://co.norton.com/security_response/.
2. Ranger, Steve. 'US intelligence: 30 countries building cyber-attack capabilities'. ZDNet, 5 Jan 2017. Accessed Oct 2017. www.zdnet.com/article/us-intelligence-30-countries-building-cyber-attack-capabilities/.
3. '2017 DOD budget calls for 15% increase in military cyber-security spending'. Military & Aerospace Electronics, 24 Feb 2017. Accessed Oct 2017. www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html.
4. McCarthy, Niall. 'The Top 15 Countries For Military Expenditure In 2016 [Infographic]'. Forbes, 24 Apr 2017. Accessed Oct 2017. www.forbes.com/sites/niallmccarthy/2017/04/24/the-top-15-countries-for-military-expenditure-in-2016-infographic/#c40fca643f32.
5. Assis, Claudia. 'This is how much it will cost to replace the Tomahawks used in Syria'. MSN, 8 Apr 2017. Accessed Oct 2017. www.msn.com/en-us/money/companies/this-is-how-much-it-will-cost-to-replace-the-tomahawks-used-in-syria/ar-BBzxyXr.
6. 'Military and Security Developments Involving the Democratic People's Republic of Korea: Report to Congress'. Office of the Secretary of Defense, 2015. Accessed Oct 2017. www.defense.gov/Portals/1/Documents/pubs/Military_and_Security_Developments_Involving_the_Democratic_Peoples_Republic_of_Korea_2015.PDF.
7. 'Alert (TA17-164A) HIDDEN COBRA – North Korea's DDoS Botnet Infrastructure'. US Cyber Emergency Readiness Team, 13 Jun 2017, revised 23 Aug 2017. Accessed Oct 2017. www.us-cert.gov/ncas/alerts/TA17-164A.
8. Park, Ju-min; Pearson, James. 'Exclusive: North Korea's Unit 180, the cyber warfare cell that worries the West'. Reuters, 20 May 2017. Accessed Oct 2017. www.reuters.com/article/us-cyber-north-korea-exclusive-idUSKCN18H020.
9. 'North Korea already has a devastating weapon: cyber-attacks'. NBC News, 15 Aug 2017. Accessed Oct 2017. www.41nbc.com/2017/08/15/north-korea-already-has-a-devastating-weapon-cyber-attacks/.