A Survey Paper: Cybergeddon

Vishakha Om. Gupta
M.Tech. Department of Computer Science and Engineering
SIST, RGPV University Bhopal-India

Arun R. Gupta
MCA, Department of Computer Science and Application GGITS, RGPV
University Jabalpur-India

Abstract:- **Cybergeddon refers to cataclysm resulting from a large scale sabotage of all computerized networks, systems and activities. It combines cyber terrorism, cyber warfare, cybercrime, and hacktivism into scenarios of wide scale internet. A new term "Cybergeddon" has been coined, relating to the potential loss of intellectual property, intelligence infrastructure and related industries dealing primarily in data exchange or storage. The target today is not a person or place, but rather a person's data or a place's significance. FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs.With the increase use of internet cybergeddon seems to be a new style of attack. Countries are having defended themselves against an increasing numbers of attacks on their information and communication system from unfriendly state, terrorists and other foreign adversaries [12]. Cyber security measure should be seen as an integral part of risk mitigation strategies, because cyber is a part of everyone's day with few exceptions. We are all connected and through our IP enable device both at home and work, these connection become ever more complex and exploitable. Part of all problem as per our survey is bit of a disconnect with security at the top of many of our organization. This is where culture is driven from and addressing this worrying knowledge gap is vital. Interconnected nature of the internet leads to the increasing danger of cyber risks. In propose paper we are trying to explore cybergeddon, future cyber war and how to prevent this.**

General Terms:- "Cybergeddon is a possibility, Attacks on critical infrastructures such as the power grid or financial institutions could wreak havoc not just on United States economy, but in fact, the world economy."

Keywords:- FBI, NSA, ARPANET.

1. INTRODUCTION

The Internet, always un-ruled and unruly, and becomes a 'failed state' in a near permanent state of disruption. Every kind of conflict is not just possible but ongoing all of the time. In the "Cybergeddon" scenario, cooperating to try to thwart attackers is either useless, as attackers always have the edge, or impossible, like trying to govern a failed state [11]. Offense continues to outpace defense, and new attacks quickly evolve to evade or overwhelm new countermeasures. The incrementally built security of many networks and the expense and difficulty of correcting security gaps for individuals and many organizations means that older attacks will continue to be successful. Inertia could take many over the cliff. In the "cybergeddon" scenarios, the Internet would still exist, but it would be a much less reliable, much more dangerous place to be especially for businesses and government agencies. Here, individuals without the skills, money, or technical resources to better secure their digital lives could get caught in the crossfire. In the worst case scenario, the initial impact from a security collapse of most public networks would be financial losses for companies who lose customer data, disruption or destruction of national infrastructure that has become dependent on the Internet, loss of the convenience of things like ATMs and online bill payment, and potentially damage to power grids and other utilities that might be targeted. Even if such systems were hardened, attacks on Internet infrastructure itself could knock critical infrastructure dependent on the Internet offline. And while disruptions like the DarkSeoul and Sony Pictures attacks wouldn't permanently damage companies [10], they could disrupt things enough to have a significant impact. More stealthy attacks like those on retailers over the last year, if accomplished on a large scale by a state actor, could do even more damage [3].

1.1 Cyber security

In a computing context, the term security implies cybersecurity. According to a December 2010 analysis of U.S. spending plans, the federal government has allotted over $13 billion annually to cybersecurity over the next five years. Ensuring cybersecurity requires coordinated efforts throughout an information system. Elements of cybersecurity include:

□ Application security.
□ Information security.
□ Network security.
□ Disaster recovery / business continuity planning.
□ End-user education.

One of the most problematic elements of cybersecurity is the quickly and constantly evolving nature of security risks. The traditional approach has been to focus most resources on the most crucial system components and protect against the biggest known threats, which necessitated leaving some less important system components undefended and some less dangerous risks not protected against. Such an approach is insufficient in the current environment [1].

The big problem is not proving some malignant software was inserted in a facility and did damage. The big problem is proving who did it. While you can trace an attack, you can also, as the attacker, leave a false trail to another location (in another country). "Network forensics" (investigating an attack and tracing where who came from where for what purpose) that will be widely accepted. At present, there are no such generally accepted criteria for proving who carried out a Cyber War attack. FBI (which is responsible for detecting and investigating Internet based crime) has been issuing increasingly scary warnings that America is becoming ever more vulnerable to "cybergeddon" (a massive attack via the Internet that would cripple the economy, government and military.) a major reason is that the threat is largely invisible. A picture of a nuclear bomb going off, or of enemy tanks and warships ready to attack makes a much more effective impression on the politicians who dole out the money. There is little consensus on exactly what the something should be, and to what degree the government should be involved. For example, Internet technology changes far more quickly than new laws can be passed to adapt and keep up. Companies fear that government interference will drive their operating costs up, while providing little, or no, protection from Cyber War attacks.

2. *Future Cyber War*

There hasn't been a proper, all out Cyber War yet. There have been lots of skirmishes, but nothing approaching what a no holds barred battle, via the Internet, would be. What would the first Cyber War be like? Let's be blunt, no one really knows. But based on the cyber weapons that are known to exist, and the ones that are theoretically possible, one can come up with a rough idea. There are three kinds of Cyber War possible.

2.1 *Limited stealth operations (LSO)*

As Chinese, Russian, and others, uses Cyber War techniques to support espionage efforts. China is the biggest practitioner, or at least they have been caught most often. But getting caught carrying out Cyber War operations does not mean you have any human prisoners, just a pile of computer forensics. The Chinese simply deny everything and carry on [7] [11].

2.2 *Cyber War only (CWO)*

This is open use of a full range of Cyber War weapons. No one has admitted doing this yet, and it's potentially less dangerous than firing missiles and unleashing tank divisions. It is believed that Russia indulged in this in 2007, when Estonia infuriated the Russians by moving a World War II statue memorializing the Soviet "liberation" of Estonia (which didn't want to be liberated by the Soviet Union.) Russia denied responsibility for the massive Cyber War assaults on Estonia, which nearly shut down the nation's Internet infrastructure. Estonia accused Russia of being responsible, and tried to invoke the NATO mutual defense pact. NATO Cyber War experts went to Estonia, and shortly thereafter the attacks stopped. Apparently Russia got the message that this sort of thing could escalate into something more conventional, and deadly. This sort of thing is being cited by the United States as a reason for coming up with "this is war" criteria. Russia again used such tactics against Georgia in 2008 and Ukraine in 2014-15.

2.3 Cyber War in support of a conventional war

Technically, we have had this sort of thing for decades. It has been called "electronic warfare" and has been around since World War II. But the development of the Internet into a major part of the planet's commercial infrastructure, takes "electronic warfare" to a whole other level. Cyber War goes after strategic targets, not just the electronic weapons and communications of the combat forces. A successful Cyber War depends on two things; means and vulnerability. The "means" are the people, tools and cyber weapons available to the attacker.

The big problem with Cyber War is that there has not been a lot of experience with it. Without that, no one is really sure what will happen when someone attempts to use it at maximum strength. But unlike nuclear weapons, there is far less inhibition about going all out with Cyber War weapons. That is the biggest danger. Cyber War is a weapon of growing might, and little restraint by those who wield it. Things are going to get a lot worse.

3. HACKER CITY

The fundamental architecture of the Internet, a decade of software rot, corporate indifference, government subversion, a flawed approach to security fixes, globalization, the increasing sophistication of criminals, the easy access to instruments of evil, and plain old human nature all of these things factor into the growing gaps in Internet defenses. The Internet still does a pretty good job getting packets around; the question is whether the packets get there securely? It's not really designed for privacy or integrity mostly resilience. Fundamentally, a city isn't the best metaphor for the Internet. Nobody's the mayor, and the only real government has been the Internet Corporation for Assigned Names and Numbers which acts more like a zoning board. But ever since it emerged from its infancy as the Defense Department sponsored ARPANET, the Internet has had the sort of basic stability associated with a city. There's crime that, despite relatively high rates, has not been left completely unchecked; a governance of sorts through some collaboration between governments, network providers, and other organizations; and relatively unrestricted and unmolested transit of communication and trade.

However, just like a city, the Internet has some neighborhoods that are safer than others. There are some places that have been neglected Windows XP slums, university and corporate networks without proper locks and poorly maintained Web servers, unlatched and neglected WordPress blogs and Windows Home Server installs. This is the Internet's "skid" row, where anybody with a little time to search can find a tool to root a server or create a bonnet. Social media has allowed people who haven't met in person have a common bond, and they can get into a group structure that allows them to have a lot more strength. [4].

Hackers at all levels have also had the benefit of learning from the big boys, or at least trying to copy their "Advanced Persistent Threat" (APT) playbook. Such methods were once the hallmark of nation state funded actors, but these are now common in attacks on retailers and other organizations. Instead of trying to force the locks, they just steal the keys by targeting specific users and then hide themselves by using multiple methods of access and covering tracks with self-destructing malware and other measures. It doesn't help that the targets of cyber attacks make it all too easy for such tactics to succeed, often without much effort. The main cause for security issues, management discipline or a lack thereof. The big problem at most organizations is that they continue to take an incremental approach to security. People always try to evolve their approach, and they're always a step behind. He compared the architecture of many organizations, based on older client and networking approaches, to a "termite infested wooden ship" just waiting to sink. And defense at many (if not most) organizations isn't even trying to keep up with current types of attack .Patches don't get applied because they're too costly to implement, because they're not a business priority, or both. It isn't even that the attack vectors have changed much; it’s the way organizations choose to deal with them. They're not ignoring them, but some have transferred the risk to an insurance aspect rather than doing the right thing with their security. That's really how the business people think. At the same time, the IT and electronics industries still push out products that include security as an afterthought, continuing to ship vulnerable versions of embedded software for years after a patch was released. Flaws in common protocols used by consumer and professional devices, such as Universal Plug and Play, make them potentially vulnerable to being hijacked by an attacker out of the box. And consumer awareness of these issues remains woefully low.

4. SURVEY PREDICTION

According to survey upcoming future of internet will be as follows.

4.1 Paradise

Security technology becomes so good that the Internet becomes an "overwhelmingly secure place." Only highly sophisticated attackers sponsored by nation states can pull anything off. Crime, espionage, and warfare against network infrastructure become very difficult

Likelihood: Low; New technologies such as cloud-based security or international cooperation could make this happen.

4.2 Status Quo

Things as they stand now: High levels of crime and espionage, but no massive cyber wars. Leading e-commerce providers continue to stay on top of attacks, fraud affects a small percentage of transactions, and criminals continue to get rich (but not too rich).

Likelihood: Moderate; Maybe there's some inherent stability in the Internet. For 15 years, people have been predicting big attacks against vital infrastructure, and none have happened yet. (Sony Pictures doesn't really count as "vital infrastructure.")[10] Defensive technologies like distributed denial of service attack protection through content delivery networks and cloud-based security infrastructure could help many organizations stave off major attacks, though the have-nots of information security would remain vulnerable.

4.3 Conflict Domain

The Internet becomes just like every physical domain of human existence: turf to fight over. Crime, espionage, embargoes, and full blown nation-on-nation conflicts extend into the Internet.

Likelihood: High; it’s happened in every other domain of human existence, and low-intensity cyber warfare has already happened. Sony Pictures proved that "soft target" companies with high profiles make excellent political targets and that the uncertainty created by attacks can be used to intimidate without the actual use of physical force [10]. Stuxnet showed that cyber weapons can have a physical effect, but it also offered a blueprint for other would be cyber warriors to follow. State sponsored or tolerated cybercrime could be used as an extension of economic warfare.

4.4 Balkanization

For security and political purposes, there is no single Internet, just a collection of national Internets. Nations are possibly blocking access to content, although there may be fewer outright attacks. Internet companies would have to duplicate infrastructure in every enclave, and surveillance would be greatly simplified for nation states.

Likelihood: Low; Countries such as China and Iran have built national firewalls, and Russia has passed a "data sovereignty" law. Others may do the same, and the effort (thus far blocked by the US and UK) to put the Internet under the regulation of the UN's ITU could exacerbate the problem [14] . In reference to Brazil's brief consideration of requiring all cloud services to keep citizens' data in that country in the wake of the Snowden spying revelations. But for now, the interconnectedness of the Internet is unlikely to be significantly reduced outside more oppressive states [3] [13].

Above scenario would have its own social and economic impact, It would greatly reduce international free speech and commerce in exchange for a modicum of security against extra national threats other than espionage and other state driven activities. If companies need different marketing plans for different countries, they might need entirely different digital infrastructures. Can we really afford separate digital infrastructure for every country that has digital borders? And if you have a large scale shock that requires countries to work together, there's not that much trust there, especially since national infrastructures are run by the national security apparatus. While the signs of future distress are certainly there, above any scenario are inevitable. The capabilities of attackers would outstrip the ability of most organizations to defend themselves has held up fairly well in the past four years. The tools and skills of attackers whether they're state-funded cyber warriors, syndicates of cybercriminals, or one in the ever changing line up of "hacktivist" groups looking to score for their cause combined with the unchecked flow of discovered security vulnerabilities have reached the point where organizations just have to assume they’ve already been hacked. A survey of over 3,000 technology professionals in 49 countries by the IT recruiter Harvey Nash Group found that 46 percent of companies worldwide had been hacked in the last year, up six percent from last year. In the US, 53 percent of companies reported being hacked. Worldwide, 52 percent of IT professionals reported being personally hacked; in the US, that figure was 55 percent. Anecdotal evidence suggests the actual numbers may be much higher; the success of hackers is not exactly shocking. In the computer security realm, attackers had an advantage early since the invention of networks.

5. HOW TO PREVENT CYBERGEDDON

- Make data security a priority. Educate employees about the importance of securing sensitive or confidential data. Implement security policies that list down recommended safety practices such as the use of strong passwords and recognizing phishing emails. Employees should exercise caution when browsing the Web and downloading applications.
- Have a backup plan for your cloud. Research cloud services before adopting them. What are the terms of service? Do they have contingencies in case of service disruptions? Prepare a backup plan in case of power outages and other service disruptions to make sure that business remains as usual.
- Install security solutions on mobile devices. Using a security solution for mobile devices ensures that the device and its data are protected from malware and other threats. Additional features like remote wipe add another layer of security as data can be erased when the device is lost or stolen.
- Be on the lookout for social engineering. It only takes a click to make your business vulnerable to different attacks and threats. The latest security intelligence can help you and your employees learn about possible scenarios or modes of attack that cybercriminals may use against your organization.
- Protect against spam and malware. The constant refinement of malware means that they remain a serious risk to any organization. Using effective anti-malware solutions can protect businesses from anyone with malicious intent [9].

6. RISK REDUCTION KEY TO TACKLING CYBERGEDDON

Businesses should tackle cyber crime by seeking to reduce risk, As companies will never be able to make cyber crime go away, there is a lot they can do to reduce the risk to the business, The reality is that companies cannot plug every potential security hole, but a proper risk assessment will help prioritize investment and plans of action. A risk-based approach will ensure that companies are more resilient, that they will be able to respond quicker to threats that really matter and that networks are properly segmented. By segmenting networks, businesses can ensure that only authorized employees are able to access appropriate data assets [8].

6.1 Restrict reach of hackers

Segmentation of networks also helps to restrict attackers if they are able to breach perimeter defenses because, without the necessary credentials, they will be limited to the segment that has been breached. If attackers are restricted in their movement once they are inside a network, it gives businesses more time to respond and limits the amount of damage the attackers can do. A lack of segmentation is a key flaw that has been identified in the Sony Pictures network, allowing attackers to have free reign once perimeter defenses had been breached. If organizations assume that they will be breached at some point, that helps to further refine the risk based priorities, Instead of focusing only on building higher, thicker walls, this approach ensures that when fireballs do come flying over the walls, the company has some water buckets ready to put out the flames. In this way, organizations become more resilient, in the sense they are better able to deal with breaches, enabling them to better understand the real extent of the attack and bounce back.

6.2 Address biggest risks first

However making cyber risk part of operational risk is not easy and, consequently, while some organizations do it well, that is not true for all. Organizations that are handling cyber risk well typically identify what particular cyber risks their particular sector and business are exposed a risk-based approach enables organizations to identify a starting point that ensures the greatest risks are addressed first. Businesses can decide what risks must be reduced, how much time and effort to spend on doing that, and what risks they can afford to live with.

6.3 Assess supplier risk

Organizations must not forget to include their supply chain in their risk assessment because, as per survey Target suppliers can be the weakest link, Security credentials stolen from an air conditioning firm that was a supplier to the US retailer were used by attackers to gain unauthorized access to Target’s network. Managing the information security capabilities of suppliers is difficult, but possible if bigger companies help smaller suppliers to improve their security posture. It may be worth considering working with and helping suppliers become compliant with your security requirements rather than relying on their assurances that they are compliant.

6.4 Share security knowledge

Any company is weaker when it stands alone, rather than sharing information with industry peers about what threats they are facing and what approaches are working well. A community based approach also enables member organizations to share resources and skills as well as threat information.

7. CONCLUSION

According to our survey, the security and safety of the Internet is going to only be solved by technology, not laws. And that's probably going to require a rip and replace of certain elements of corporate and public networks to make happen. But unless there's some sudden transformational moment, there will always be a long tail of vulnerable devices and systems connected to a network that attackers can exploit in some way. Internet Protocol version 6 was supposed to solve many of these problems, but most of the world is still on IPv4; Windows as a service may fix many computers, but there are still millions running Windows XP.There's only one thing that's guaranteed at this point; the computer security community won't be facing a job shortage anytime soon.

8. REFERENCE

[1] Osorio, F.C.C. ; Leitold, F. ; Mike, D. ; Pickard, C. ; Miladinov, S. ;Arrott, A. 2013. Measuring the effectiveness of modern security products to detect and contain emerging threats a consensus-based approach.

[2] Fletcher, K.K. ; Xiaoqing Liu .2011. Security Requirements Analysis, Specification, Prioritization and Policy Development in Cyber-Physical Systems.

[3] Leo, M. ; Battisti, F. ; Carli, M. ; Neri, A.2014. A federated architecture approach for Internet of Things security Euro Med Telco Conference (EMTC).

[4] Feily, M. ; Shahrestani, A. ; Ramadass, S.2009. A Survey of Botnet and Botnet Detection.

[5] Sitnikova, E. ; Asgarkhani, M. 2014. A strategic framework for managing internet security Fuzzy Systems and Knowledge Discovery (FSKD), 2014 11th International Conference.

[6] Redford, M. U.S. and EU.2011. Legislation on Cybercrime Intelligence and Security Informatics Conference (EISIC), 2011 European.

[7] Naqvi, S. ; Dallons, G. ; Ponsard, C. 2010. Applying Digital Forensics in the Future Internet Enterprise Systems - European SME's Perspective.

[8] Hooper, E. 2009. Intelligent strategies and techniques for effective cybersecurity, infrastructure protection and privacy Internet Technology and Secured Transactions, 2009. ICITST.

[9] Govil, J. ; Michigan Univ., Ann Arbor; Govil, J.2007. Ramifications of cyber crime and suggestive preventive measures.

[10] http://en.m.wikipedia.org/wiki/sony_pictures_entertainment_hack.

[11] http://www.strategypage.com/htmw/htiw/articles/20150121.aspx.

[12] http://www.encyclo.co.uk/meaning-of-Cybergeddon.

[13] http://www.usatoday.com/story/news/world/2015/02/23/ukraine-says-pullback-delayed/23871975/

[14] http://www.bbc.co.uk/news/world-europe-30907443