Nigerian Journal of Technology (NIJOTECH)
Vol. 36, No. 4, October 2017, pp. **1174 – 1183**

Print ISSN: 0331-8443, Electronic ISSN: 2467-8821
www.nijotech.com
http://dx.doi.org/10.4314/njt.v36i4.26

ZERO DAY EXPLOITS AND NATIONAL READINESS FOR CYBER-WARFARE

A. E. Ibor*
DEPT. OF COMPUTER SCIENCE, CROSS RIVER UNIVERSITY OF TECHNOLOGY, CALABAR, CROSS RIVER STATE NIGERIA
E-mail address: *ayei.ibor@gmail.com*

ABSTRACT
A zero day vulnerability is an unknown exploit that divulges security flaws in software before such a flaw is publicly reported or announced. But how should a nation react to a zero day? This question is a concern for most national governments, and one that requires a systematic approach for its resolution. The securities of critical infrastructure of nations and states have been severally violated by cybercriminals. Nation-state espionage and the possible disruption and circumvention of the security of critical networks has been on the increase. Most of these violations are possible through detectable operational bypasses, which are rather ignored by security administrators. One common instance of a detectable operational bypass is the non-application of periodic security updates and upgrades from software and hardware vendors. Every software is not necessarily in its final state, and the application of periodic updates allow for the patching of vulnerable systems, making them to be secure enough to withstand an exploit. To have control over the security of critical national assets, a nation must be "cyber-ready" through the proper management of vulnerabilities and the deployment of the rightful technology in the cyberspace for hunting, detecting and preventing cyber-attacks and espionage. To this effect, this paper discusses the implications of zero day exploits and highlights the dangers posed by this cankerworm for an unprepared nation. The paper also adopts the defence-in-depth strategy for national readiness and a foolproof system that enforces the security of critical national infrastructure at all levels.

Keywords: *exploits, zero day, vulnerability, cyberspace, cyber-warfare*

1. INTRODUCTION
The cyberspace of nations and states across the globe has witnessed a plethora of cyber incidents in recent times. Espionage and cyber warfare are becoming more prevalent as the security posture of nations and states is continuously being tested. The quest for supremacy on the cyberspace is gaining momentum as new attack vectors evolve. Stuxnet, ramnit, polymorphic worms, flame, ransomware, and the like, are typical examples of threats that trigger numerous incidents in the cyberspace. Some of these cyber incidents are perpetrated using detectable operational bypasses such as the non-application of security updates and upgrades. Software and hardware vendors periodically release periodic updates and upgrades as a means of making their products foolproof. However, security updates are released only for identified vulnerabilities in a software or hardware product. When such vulnerabilities are not detected early enough, they can pose serious security concerns for any nation. When no prior information is available for certain vulnerability, and such vulnerability is exploited by a malicious user, a zero day exploit is inevitable.

In [1], it is asserted that a zero day exploit means zero day of awareness and as such so much damage can be done. Similarly,[2] and [3] opined that a zero day exploit such as a polymorphic worm has the capacity to trigger unpredictable network behaviour over the Internet. According to [4], zero day exploits are threats to information assurance. Furthermore, Li et al in [5] asserts that the wild proliferation of zero day exploits especially zero day polymorphic worms is an emerging threat for the cyberspace. These threats include and are not limited to unauthorised access to classified contents, theft of digital assets and business intelligence, infestation of critical systems with viruses, worms, Trojans, rootkits and backdoors as well as prevalent system crashes and loss of revenue. In a recent development in Nigeria, it was reported that about ₦127 billion, representing 0.08% of the country's Gross Domestic Product (GDP) is lost annually to

* **Author tel: +234 – 703 – 081 – 6869**

cybercrime. This is just a case in point as several other nations and states are being drained of their respective revenues from cybercrimes, some of which are zero days.

Responding to a zero day has posed to be a significant task. Since no known patch or fix is available at the time of a zero day exploit, it is pertinent to have an efficient security framework that can reduce its impact. Having a robust security framework or architecture comes with strategic planning that is a product of national readiness for any cyber-aware nation. The situation of an unready nation may as well be characterised by frequent cyber incidents, which are likely to compromise the confidentiality, integrity and availability of critical national infrastructure. In response to these challenges, this paper proposes an approach based on defence-in-depth for limiting the impact of zero days to the attack zone. This containment is necessary for protecting critical assets and truncating the escalation of the impact of zero days to allow for quick recovery by nations and states.

2. THE CYBERSPACE AND NATIONAL CRITICAL INFRASTRUCTURE

The cyberspace is a community of connections in which networks interact across distances to allow for the sharing of data, information and programs. The seamless nature of the cyberspace has come as a blessing and a huge security concern as well. While data and information sharing has enabled the expansion of the Internet and digital communications, it has also become the stimulant for security breaches and diverse cyber incidents over the years. Considering the intricate nature of the cyberspace, nations and states have in one way or the other been involved in enacting laws, regulations and documenting policies for controlling the use of the cyberspace, and ensuring a possible zero-violation of its digital assets and network contents. However, the challenge is expanding on a daily basis. New applications are being developed, and this development comes with more security issues.

New trends in cloud computing provides for easy access to data anywhere and anytime. Nations and governments have imbibed this ease of access, and many are yet to consider the security implications of this shared pool of computing resources. Most affairs of government have now been migrated to the cyberspace. E-commerce, e-governance, e-banking, and other electronic platforms are gradually replacing the traditional manual processes in all spheres. Migrating access to classified data and critical national infrastructure to the cyberspace requires a robust security architecture.

The cyberspace serves as a parallel universe of computers and digital communications, providing access to data and information at very high speeds [5]. The question of migrating the transactions and operational routines of nations and states to the cyberspace is no longer controvertible as the Internet has found widespread relevance owing to its virtual proximity, availability, ease of access, and flexibility in the context of data and information sharing. To this effect, [6] shares the view that the heavy reliance of critical infrastructures and enterprises on computer networks must have concomitant hardened security architecture that is measurable and feasible. This hardened security standpoint is aimed at truncating intrusions targeted at networks and connected computer systems. The development of such a security framework should begin with a comprehensive risk assessment of the internal and external factors that can militate against national security infrastructure. A nation must be able to assess its current state of defences, and ensure a periodic review of these defensive strategies to allow for the identification and documentation of potential threats to its cyberspace.

Having a comprehensive documentation of the potential risks that can plague a nation's infrastructure can begin with a national database of vulnerabilities. The National Vulnerabilities Database (NVD) of the United States is a clear demonstration of the need to assemble databases of security checklists, security related software flaws including misconfigurations, product names, and impact metrics [7]. Mobile device evolution, and the miniaturisation of computing devices paved way for new software applications to evolve with added security concerns. Most government formations also allow employees to bring their own devices to access privileged data and applications, raising concerns of the privacy of classified contents. The totality of these security issues, have over the years, had tremendous impact on the cyberspace including the confidentiality, integrity, and availability of services over a national infrastructure.

The cyberspace has become a breeding ground for cyber-warfare. The transition from the physical objects of communication to the use of electronic means with the added advantage of anonymity provides a platform for possible cyber-warfare and other cyber-related offences. As discussed in [8],there is a casual relationship between the cyberspace and cyber objects. This relationship triggers the existence of cyber-spatial objects, which are addressable, and as such can be

accessed legitimately or otherwise. Accessing these contents without prior authorization is the basis for continuous security breaches across the cyberspace. Furthermore, Luker in [9] discussed the various implications of insecure cyberspace, and proposed strategies for reducing the possible debilitating effect of threats in the cyberspace, mentioning that the challenge of a secure cyberspace is based on a concerted, coordinated and focused effort from all levels of government, including the private sector and individuals.

Cyber-systems support most national critical infrastructures across the globe [10]. The security of these infrastructures including the confidentiality, integrity, and availability of digital assets owned by the government, organisations, institutions, and individuals depends on the strategies deployed by nations and governments to protect the cyberspace. The enactment and adherence to regulations and laws pertaining to the use of the cyberspace can as well leverage the severity of cyber incidents. The computer misuse act of the United Kingdom in [11], the regulation of investigatory powers act in [12], the computer fraud and abuse act in [13], as well as the Nigeria Cybercrimes Act in [14], are documented regulations in the public domain that detail the acceptable standards for using and distributing computing resources, and the penalties associated with them. These regulations are necessitated by the controlled use of the cyberspace, and subsequent protection of critical national infrastructure.

A critical look at the conceptual view of the cyberspace, as shown in Figure 1, shows that the interdependency of the various components constituting the physical, logical and information layers including the users represent a seamless interaction that requires a robust security standpoint to mitigate the proliferation of cyber threats in recent times. Since every user that is connected to the cyberspace can in one way or the other influence the "health" of cyber systems, which may or may not support the interactions within critical infrastructure, being proactive in proffering solutions to the ravaging effect of the erratic nature of the cyberspace is key to degrading the effect of zero day exploits.

Figure 1 depicts the interactions between the various components of the cyberspace at a high level of abstraction. The users, who actually define the nature and structure of the cyberspace, also influence its usage and popularity. Access to digital assets, including the possible abuse of these assets, services rendered and the technology driving the communication infrastructure on which all connections originate and terminate depend on the human factor. Technology driven solutions to the security of cyberspace can also be compromised by the human factor. Consequently, enforcing a secure cyberspace must be based on a multi-level security architecture that is computationally expensive to circumvent while restraining possible impacts of zero days to the attack zone.

3. EXPLOITING THE THREE DIMENSIONS OF THE CYBERSPACE

The components of the cyberspace can be considered in three dimensions. One dimension of the cyberspace is in relation to the network of computers that form the basis for interconnectivity between people. This interconnectivity has the goal of information sharing through the cyberspace and has also been the tool for the spread of all categories of malware. Viruses, worms, Trojans, rootkits, backdoors and ransomware are propagated and escalated through the interconnectivity of the network of computers including the sharing of information through methods such as the use of pen drives.

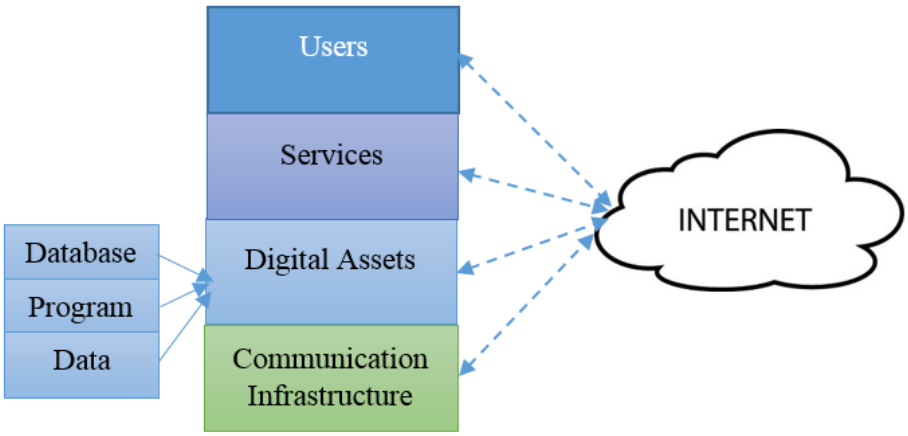

Figure 1: A conceptual view of the cyberspace

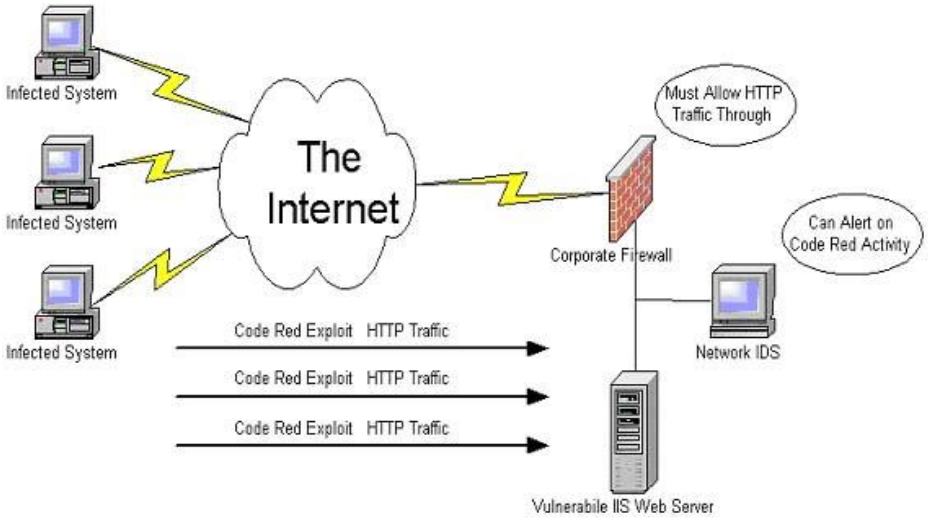

Figure 2:Denial of Service attack caused by Code Red (CRv2) [18]

The impact of a zero day exploit that is used to hijack a network of computers can have fatal consequences on the lives of the people being linked through the network. The disclosure of classified data and programs such as the Panama Papers [15], in which a zero-day flaw in Drupal content management system is now being said to be responsible for hackers penetrating the network of the law firm Mossack Fonseca to extract more than 11.5 million files, culminating in the theft of about 2.6 terabytes of data, and further modification or distortion of the data and programs against a nation will have even more drastic effect on the economy of such a nation.

Computers that are connected through a network depend on the processes and actions initiated by people to establish a contents-base, populated with all classes of information, which can be accessible by anyone with an Internet-enabled device from anywhere in the globe. However, this information resides on machines such as servers, laptops, personal computers, and smartphones.

The machines, which are basically manipulated by people constitute the second dimension of the cyberspace. In a typical attack scenario, machines are pivotal to the success of an attack including a zero day exploit. A vulnerability exploited by an attacker can be used to hijack a machine to the extent of using it as a pivot for illegally penetrating and maintaining access to other machines. In a Distributed Denial of Service (DDoS) attack, a malicious user can make use of computers of other users (usually vulnerable hosts in a network) to stage an attack against another computer or network. These vulnerable hosts can be discovered through the extensive scanning of networks. Resources such as bandwidth, memory, computing power and operating system data structures can be affected by a DDoS attack. Three of the scanning techniques that can be used as stated in [16] are discussed as follows:

3.1 Random scanning

This involves the random probing of the IP address space by an infected machine, which may be the attacker's machine or a collaborating machine (usually called a zombie) to discover and infect vulnerable machines. In this way, the infected machine spreads its malicious code, completely taking control of other machines and causing them to spread the malicious code to other vulnerable machines [17]. Code Red (CRv2) worm is an example of a malware that spreads through random scanning. As shown in Figure 2, it is possible for the Code Red exploit to permeate HTTP's default port (TCP port 80) even with a corporate firewall installed. The firewall will have no protection against this exploit since most firewalls can allow HTTP traffic through. An IDS (intrusion detection system) can trigger an alert indicating the presence of a code red exploit.

3.2 Hit-list scanning

In this technique, a pre-acquired list of IP addresses of machines that may be vulnerable is used to scan and infect matched vulnerable machines. This trend continues to install malicious code on more and more vulnerable machines within a short span of time as the scan progresses.

3.3 Permutation scanning

In each machine, there is a pseudorandom list of IP addresses acquired through permutation, which can be constructed with a 32-bits block cipher using a predetermined key. The infected machine scans at random positions in a well-coordinated way such that

already infected machines can be easily identified. In this way, the scanning is faster, and performs better for a large pool of IP addresses. Partitioned permutation scanning combines the techniques of hit-list and permutation scanning respectively, such that whenever a compromised host is found, the hit-list is divided into two equal parts. One half of the list is assigned to the new target, which proceeds in the same manner to infect other machines in the list until all vulnerable targets are located and infected.

The second dimension of the cyberspace, proves to have enormous impact on the cyberspace including the tendency to initiate cyber-warfare as well as the ability to protect the cyberspace from intruders. All programs and data are hosted on machines. These programs and data are prone to vulnerabilities that are exploitable. A search for vulnerabilities based on software flaws between January 2010 and October 2016 as contained in the National Vulnerability Database of the United States with the Common Vulnerability Scoring System (CVSS) version 3 returned a total of 38, 956 vulnerabilities [19]. Although there may be a slight drop in the number of vulnerabilities in 2016 as compared to 2014 and 2015 respectively, the huge number of vulnerabilities poses significant security risks to corporate and small scale businesses, organisations, institutions, governments of nations, industries and companies across the globe. The evidence of the reality of threats to computer infrastructure from both internal and external sources is an issue that requires adequate measures for mitigation.

Representing these figures using a line graph as shown in Figure 3, reveals that there is still much to be done as a means of creating highly secure environments for the various parties that deliver some applications and services over the Internet as well as on local area networks.

The security of machines is largely impacted by the severity of vulnerabilities characterizing the programs run on these machines. The CVSS as proposed by the National Institute of Standards and Technology (NIST) of the United States ranks this severity as low, medium or high. Vulnerabilities ranked high are likely to allow an intruder to create a botnet (or zombie army), in which case, Internet-connected machines are able to pass messages to one another through command and control (C&C) to the extent of triggering a cyber-warfare. Between 2001 and 2016, NIST catalogued and ranked a number of vulnerabilities based on CVSS severity [20].

Botnets, which are a network of compromised computers controlled remotely, raise concerns on the security posture of critical infrastructure, and may as well spell doom for any nation that does not have a robust security framework for mitigating cyber threats culminating from the exploitation of these vulnerabilities. Similarly, an Internet security threat report (ISTR) by the Symantec Corporation in 2014 also showed a significant rise in zero-day vulnerabilities in 2013 [21]. The data reveals that exploits in the wild were capable of escalating zero-day attacks before mitigation can be proffered. It was reported that the majority of the annual total of zero-day vulnerabilities in 2013 exploited Java, a popular programming language and platform with an average exposure-window of 3.8 days. Subsequently, the users were exposed to the zero-day vulnerabilities for 19 days, leaving room for a lot of attacks to be successfully carried out.

The third dimension of the cyberspace that can pose a major security risk to critical national infrastructure is the totality of objects such as sources of information. Information sources such as websites, blogs, personal pages and accounts, emails, and a plethora of others can equip the attacker with the rightful details to circumvent the security of critical infrastructure. To this end, sensitive information posted online either intentionally or otherwise should be scrutinised for possible absence of security details. A conceptual model of the three dimensions of the cyberspace is depicted in Figure 7.

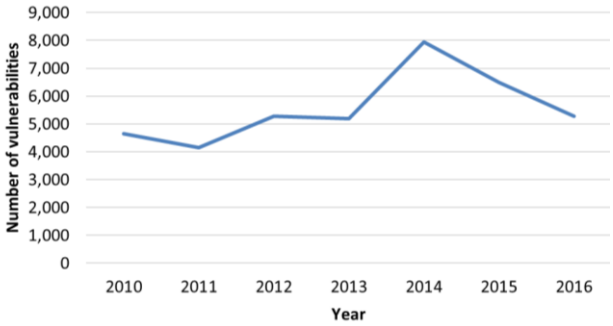

Figure 3: Line graph showing the number of catalogued vulnerabilities based on software flaws between 2010 and 2016 as reported by NIST.

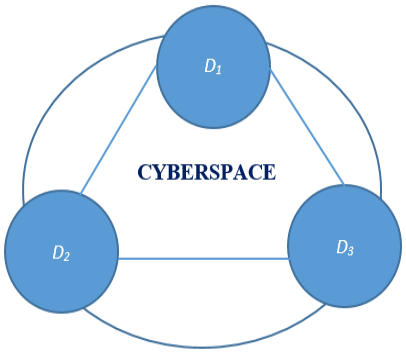

Figure 4: A conceptual model of the three dimensions of the cyberspace

In Figure 4, D_1represents the network of computers that link people across the globe to enhance information sharing; D_2 represents the machines that house the programs and data being accessed, manipulated and processed such as servers, personal computers, laptops, personal digital assistants (PDAs), smart phones; and D_3 depicts the sources of information such as websites, blogs, email accounts and so on. If therefore, every component of the dimensionality of the cyberspace is exploitable, it is important to be cyber-aware through national readiness in order to hunt, detect, mitigate and truncate zero day exploits on a nation-state cyberspace.

4. CYBER-WARFARE AND NATIONAL READINESS

The expansion on the dependence of nations on computer networks and software, owing to the high rate of industrialization and automation, creates an environment of seamless connectivity between nations and states. Content sharing in the cyberspace also considers the sharing of malicious contents. It is a possibility, in today's information era, to have conflict between nations being escalated through the cyberspace. Some examples of these include:

i) Russia-Estonia distributed denial of service (DDoS) attacks [22].
ii) The use of botnets during the Russia-Georgia war of 2008; Iran Stuxnet worm attack in 2010 [23].
iii) Night dragon targeted attacks on energy companies resulting in the theft of sensitive intellectual property [24].
iv) WannaCry and Petya ransomware attacks on high-profile targets in Europe, Asia and America [25 – 27].

The stuxnet worm is reported to have been instrumental to several security breaches that have degraded the functionality of critical national infrastructure [28]. Cyber-warfare may result from provocation, the sheer intent to perpetrate a criminal activity and/or the demonstration of cyber power by individual hackers, hacktivist groups, corrupt businesses, terrorists or nation. In each case, an attack on a computer system or network is staged in a bid to take advantage of vulnerable computer systems and software in order to propagate information theft, illegal financial gains, information distortion, or sheer sabotage.

Cyber-warfare does not rely on the physical distances between targets, and as such depends on the attacker's or defender's ability to have control over the other's cyberspace. As discussed in [29], the tools and techniques required to start a cyber-warfare can be available to both the attacker and the defender, and requires no forced entry [30]. One of such tools is strongly connected to zero-day vulnerabilities and a prolonged window of exposure for which patches of vulnerabilities are released, made public and installed. This implies that the attacker can also be the defender and vice versa. Based on this provision, each nation/state must have the security architecture necessary to protect the area of cyberspace that controls cyber systems, which support critical national infrastructure. The cyberspace is an enabling and virtual environment for cyber power. In other words, exerting influence on the cyber systems of nation-state can be made possible through the capacity to exploit the cyberspace of others to one's advantage [10]. This exploitation has already begun, and fast becoming a fifth domain in warfare outside the conventional domains of land, sea, air and the outer space.

The composition of the critical infrastructure of nations and states cut across all sectors including telecommunication, energy, food, water, emergency services, banking finance, and many more. These sectors interact through various means of communication, major of which is the cyberspace. In a real sense, the successful hijack of a nation-state cyberspace clearly interprets to the defeat of such a nation in cyber-warfare. This probable defeat can trigger a chain reaction that will include but not limited to the obliteration of financial systems, loss of trust from investors and onward economic misfortunes such as recession, stagnation and strangulation of economic policies, national technology system failures and crashes, data leaks, and loss of profits. However, enforcing a national readiness strategy through defence-in-depth may likely serve as a panacea for controlled access and isolation of the impact zone in the event of a zero-day [31], [32]. This helps to ensure that the failure of a single control does not result to total system compromise.

4.1 National Readiness through Defence-In-Depth

The defence-in-depth strategy delivers security at different levels of protection and implementation as discussed in [33], [34], and [35].Preparing for zero-day exploits and possible cyber-warfare requires a strategic plan, which must be implemented at different phases of the security architecture of every nation-state that is keen on a secure cyberspace. Different levels of security as shown in Figure 5implies protection at different layers. When security is delivered at different interacting layers of a nation's security standpoint, it is possible to isolate a certain layer of impact in the event of an exploit and truncate the escalation of an attack in real time [36].

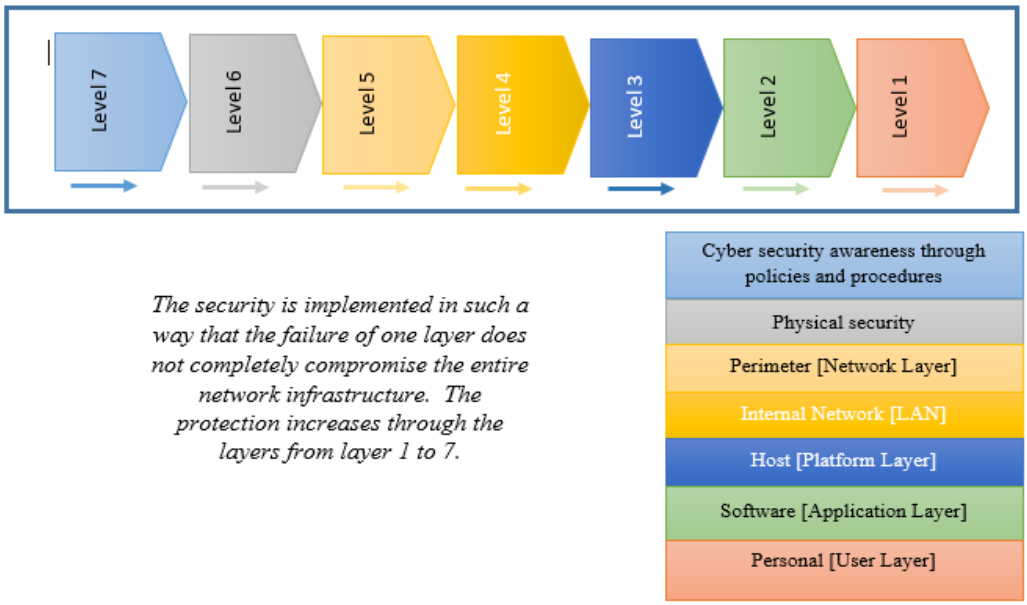

Figure 5: National readiness through defence-in-depth strategy

As depicted in Figure5, security should start at *Level 7* with awareness through policies and procedures. Government legislation should accommodate more inclusive policies that comprise of frequent awareness programmes for all levels of individuals, groups, organisations, parastatals, institutions and government agencies. Procedures for the initiation and enforcement of cyber security policies should be based on the collaboration of the private and public sectors. All documentations and regulations for strategising the defence of the cyberspace should be accessible and made available to all stakeholders of the public and private sectors, with instructions to extend the awareness to all those involved in governmental and non-governmental affairs.

Level 6 includes the physical security component of defence-in-depth. This physical security component comprises the use of closed circuit television (CCTV), locks, personal identity verification credentials, biometrics, disaster recovery and continuity of operations plan, and security personnel. The physical security should be instituted in every environment housing critical national infrastructure. This security standpoint at the physical level should be able to protect computer servers, hard and tape drives, network switches and routers, power grid, and cooling systems. It is pertinent to note that the data targeted by an attacker is stored on the tangible aspects of computing, and the protection of these tangible devices and equipment is essential for enhancing a well-formed defence-in-depth strategy.

At *Level 5*, the perimeter (network layer) is composed of boundary routers, network intrusion detection and prevention systems (Network IDPS), firewalls, virtual private networks (VPNs), proxy servers, gateway antivirus system, and remote authentication dial-in user service (RADIUS). These components help to establish connection from an information technology (IT) infrastructure to another one, possibly external partners, users or the Internet. The components should have hardened security configurations to withstand external influences such as attempts at attacks and possible attacks on the internal critical infrastructure.

At *Level 4*, the internal wired or wireless network requires server antivirus systems, network-level authentication, encryption schemes, network access protection, firewalls, time-based passwords and tokens, port security, MAC address filtering, use of static IPs, virtual local area networks (VLANs), departmental security policies, and risk management plans.

At the host layer *(Level 3)*, several strategies can be deployed to enforce a robust security posture. Some of these include the use of host-based intrusion detection and prevention systems (IDPS), server antivirus, antispyware and certificates, patch management plans, host-based antivirus and antispyware systems, data encryption schemes, and time-based passwords and tokens.

Level 2 is significantly the software or application layer. In this layer, database security, input validation schemes, web service security, data encryption schemes, application proxies and identity management

schemes must be robust to achieve a formidable security architecture.

The innermost layer, which is at *Level 1* constituents the personal or user layer. This layer contains a large collection of users that have direct contact with the data being stored and transmitted. Since data, including files, documents, databases, and configuration settings, is the primary target of the attacker, and this layer provides the basis for comprehensively protecting data from all degrees of security breaches, it is necessary to ensure that it is computationally infeasible for an attacker to penetrate the cyber systems of critical national infrastructure to the extent of having illegal access to data or the control of it in any form possible. Security components at this point should include the use of authentication and authorization mechanisms, security clearances, private key infrastructure, role and rule-based authentication, dual-factor authentication, biometric authentication such as the use of fingerprint, palm, and iris authentication as well as data encryption schemes.

Let us depict national readiness for cyber-warfare as some variable *NR*, and the layers of defence-in-depth as L_i; with i defined as $(1 \leq i \leq 7)$, then we can define *NR* as follows:

$$NR := L_i(L_{i-1})!$$

Considering this definition, it follows that there is a component-wise relation between the different layers of the defence-in-depth strategy such that every layer is defined reductively in terms of the other, with the outer layers ringed around the inner layers in a logical hierarchy. Since these multiple and overlapping layers are logically defined, it means there is the tendency to define them recursively with respect to the outermost layer. This forms a strong security outpost that can be sufficiently useful for the security of nation-state cyber systems and the corresponding safety of the cyberspace.

5. CONCLUSION

The cyberspace of nations and states is supported by cyber systems, which are constantly being threatened by zero days and cyber-warfare. The current trend of attacks makes it possible to direct thousands of malicious payloads towards critical infrastructure, thereby causing unprecedented disruption of services, data leaks, theft of digital assets, and possible modification of execution codes and process controls. Stuxnet, DDoS, botnets, Night dragon, Aurora, WannaCry, Petya and several flavours of advanced persistent threats (APTs) have been used against nation-state infrastructure. The success of these attacks have been largely due to the exploitation of vulnerabilities in software and hardware systems. Although there may be several mitigations against these exploits, the impact, sometimes, is hard to contain due to the poor security architecture of most national and state governments.

Protecting a nation's cyberspace can be effected in several ways. However, the capacity to isolate a cyberattack is based on the extent to which the possibility of the attack is reduced drastically through several layers of defences. Developing a security posture that makes it computationally infeasible for an attack to succeed in real time should be a consideration by every nation-state. Defence-in-depth, with multiple layers of security has the provision to allow for incremental security defences that can withstand malicious attacks through threat modeling, continuous risk analysis, early detection and isolation of the impact zone, the implementation of the defence-in-depth strategy as well the monitoring and reviewing of the existing security infrastructure, and creating room for improvements.

The layered structure of defence-in-depth shows that the outer security layers must be defeated before access can be allowed to the inner layers, and possibly to data, which is the core component of every critical infrastructure. The difficulty in establishing this access to critical data, constituting the established contents of the infrastructure, implies the security instituted is robust enough to keep intruders at bay. When a nation-state is able to achieve this feat, it becomes the beginning of more secure cyber systems that are able to support a safer cyberspace, and enhance the confidentiality, integrity and availability of digital assets across various critical infrastructure.

6. REFERENCES

[1] Bilge, L. and Dumitras, T., October. Before we knew it: an empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security* (pp. 833-844). ACM. 2012,

[2] Kaur, R. and Singh, February. Efficient hybrid technique for detecting zero-day polymorphic worms. In *Advance Computing Conference (IACC), 2014 IEEE International* (pp. 95-100). IEEE, M., 2014.

[3] Li, Z., Sanghi, M., Chen, Y., Kao, M.Y. and Chavez, B, May. Hamsa: Fast signature generation for zero-day polymorphic worms with provable attack resilience. In *2006 IEEE Symposium on Security and Privacy (S&P'06)* (pp. 15-pp). IEEE., 2006.

[4] Crandall, J. R., Su, Z., Wu, S.F. and Chong, F.T., November. On deriving unknown vulnerabilities from zero-day polymorphic and metamorphic worm exploits. In *Proceedings of the 12th ACM conference on Computer and communications security* (pp. 235-248). ACM, 2005.

[5] Benedikt, M., October. Cyberspace: some proposals. In *Cyberspace*(pp. 119-224). MIT Press, 1991.

[6] Wang, L., Jajodia, S., Singhal, A. and Noel, S., September. k-zero day safety: Measuring the security risk of networks against unknown attacks. In*European Symposium on Research in Computer Security* (pp. 573-587). Springer Berlin Heidelberg, 2010.

[7] Zhang, S., Caragea, D. and Ou, X, August. An empirical study on using the national vulnerability database to predict software vulnerabilities. In*International Conference on Database and Exp.*, 2011.

[8] Bryant, R. What kind of space is cyberspace. *Minerva-An Internet Journal of Philosophy*, *5*, pp.138-155., 2001.

[9] Luker, M. A. The national strategy to secure cyberspace. *Educause Review*, *38*, pp.60-60., 2003.

[10] Kuehl, D. T. From cyberspace to cyberpower: Defining the problem.*Cyberpower and national security*, pp.26-28, 2009.

[11] Walton, R. The Computer Misuse Act. *information security technical report*, *11*(1), pp.39-45., 2006.

[12] Akdeniz, Y., Taylor, N. and Walker, C. Regulation of Investigatory Powers Act 2000 (1): Bigbrother.gov.uk: State surveillance in the age of information and rights,[2001]. *Criminal Law Review*, pp.73-90, 2001.

[13] Skibell, R. Cybercrimes & misdemeanors: A reevaluation of the computer fraud and abuse act. *Berkeley Technology Law Journal*, pp.909-944., 2003.

[14] Ojo, O.V.. An Assessment of Nigeria's Cybercrimes (Prevention, Prevention Etc.) Act 2015. *The Lawyers Chronicle, The Magazine for the African Lawye*, 2015.

[15] Wikipedia (2016). The Panama Papers. Available at https://en.wikipedia.org/wiki/Panama_Papers. Accessed 18 October 2016.

[16] Cisco (2013) *Distributed denial of service attacks*. Available at: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-4/dos_attacks.html (Accessed: 15 April 2013).

[17] Colajanni, M., Marchetti, M. & Messori, M. "Selective and early threat detection in large networked systems", *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on,*p604-611, 2010.

[18] Boyce, R. *Malware FAQ: Code red - ISS buffer overflow*. Available at: http://www.sans.org/security-resources/malwarefaq/code-red.php (Accessed: 15 April 2013) 2013.

[19] NIST National Vulnerability Database Statistics. Available at https://web.nvd.nist.gov/view/vuln/statistics-results?adv_search=true&cves=on&pub_date_start_month=0&pub_date_start_year=2010&pub_date_end_month=9&pub_date_end_year=2016&cvss_version=3. Accessed 15 October 2016.

[20] NIST CVSS severity distribution over time. Available at https://nvd.nist.gov/visualizations/cvss-severity-distribution-over-time. Accessed 16 October 2016.

[21] Symantec Corporation Internet Security Threat Report. Available at http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf. Accessed 6 October 2016. 2014.

[22] Chen, T. M., Stuxnet, the real start of cyber warfare? [Editor's Note].*IEEE Network*, *24*(6), pp.2-3, 2010.

[23] Farwell, J. P. and Rohozinski, R.. Stuxnet and the future of cyber war.*Survival*, *53*(1), pp.23-40. , 2011.

[24] Cyberattacks, G. E.,. Night Dragon. *McAfee Foundstone Professional Services and McAfee Labs*. 2011.

[25] Le Guernic, C. and Legay, A., April. Ransomware and the Legacy Crypto API. In *Risks and Security of Internet and Systems: 11th International Conference, CRiSIS 2016, Roscoff, France, September 5-7, 2016, Revised Selected Papers* (Vol. 10158, p. 11). Springer 2017.

[26] Richardson, R. and North, M. Ransomware: Evolution, Mitigation and Prevention. *International Management Review*, *13*(1), p.10, 2017.

[27] Martin, G., Kinross, J. and Hankin, C.,. Effective cybersecurity is fundamental to patient safety, 2017.

[28] Kerr, P. K., Rollins, J. and Theohary, C.A., 2010. *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability* (pp. 1-9).

Washington, DC: Congressional Research Service. , 2010.

[29] Parks, R. C. and Duggan, D. P.. Principles of cyberwarfare. *IEEE Security & Privacy Magazine*, *9*(5), pp.30-35, 2011.

[30] Libicki, M. C.,. *Conquest in cyberspace: national security and information warfare*. Cambridge University Press 2007.

[31] Kuipers, D. and Fabro, M.. *Control systems cyber security: Defence in depth strategies*. United States. Department of Energy, 2006.

[32] Lippmann, R., Ingols, K., Scott, C., Piwowarski, K., Kratkiewicz, K., Artz, M. and Cunningham, R., October. Validating and restoring defence in depth using attack graphs. In *MILCOM 2006-2006 IEEE Military Communications conference* (pp. 1-10). IEEE, 2006.

[33] Stouffer, K. K. and Falco, J. Recommended practise: Improving industrial control systems cybersecurity with defence-in-depth strategies. *Department of Homeland Security, Control systems security program, national cyber security division,* 2009.

[34] Jajodia, S., Noel, S., Kalapa, P., Albanese, M. and Williams, J., , November. Cauldron mission-centric cyber situational awareness with defence in depth. In *2011-MILCOM 2011 Military Communications Conference* (pp. 1339-1344). IEEE, 2011.

[35] Bass, T. and Robichaux, R.. Defence-in-depth revisited: qualitative risk analysis methodology for complex network-centric operations. In *Military Communications Conference, 2001. MILCOM 2001. Communications for Network-Centric Operations: Creating the Information Force. IEEE* (Vol. 1, pp. 64-70). IEEE, 2001.

[36] Byres, E., Defence in depth. *Control Engineering Asia* June 2008.