Mladenovi, Dragan D.
Vulnerability assessment and penetration testing in the military and ihl context
Vojnotehnicki glasnik/Military Technical Courier, vol. 65, núm. 2, 2017, pp. 464-480
University of Defence

ПРЕГЛЕДНИ ЧЛАНЦИ
ОБЗОРНЫЕ СТАТЬИ
REVIEW PAPERS

VULNERABILITY ASSESSMENT AND PENETRATION TESTING IN THE MILITARY AND IHL CONTEXT

Dragan D. Mladenović
Serbian Armed Forces, General Staff,
Department of Telecommunications and IT (J-6),
Belgrade, Republic of Serbia,
e-mail: dragan.mladenovic@vs.rs,
ORCID iD: http://orcid.org/0000-0003-4530-633X

Abstract:

Vulnerability assessment and penetration testing are the key activities of information security risk management and cyber defense and intelligence done by military organizations. These activities are significant not only in the context of performing military operations, but also in the International Humanitarian Law (IHL) and law enforcement contexts. The application of information technologies in the military and civilian environments increases complexity in the field of risk management. Besides information security, military organizations have the task to undertake necessary activities in the fields of cyber operations, both for defense and offense purposes. They depend on technologically based knowledge and skills and are implemented by specific organizations within military systems. The goal of vulnerability assessment is to discover and determine the nature of vulnerabilities, without considering how they may be used for offense, while penetration testing uses exploits for breaching into systems and thus estimates the type and degree of risk these vulnerabilities represent to the system. However, even if they represent two different activities, with different end goals but the same field of interest, they are complimentary and inter-dependent. Since their common feature is development of knowledge and skills based on the same technologies, they are equally important both for risk management, military operations in cyberspace and their use for defense and intelligence activities as well as for IHL.

Key words: vulnerability assessment, penetration testing, cyber attack, International Humanitarian Law.

Introduction

Significance and influence of information technologies in all modern organizational and technical systems is obvious and ever growing. Military organizations require application of reliable and efficient technical systems for performance of their basic function – defense, both in peace time and during war. In modern armies, such characteristics are mostly enabled by the application of independent and embedded information technologies. No matter whether these technologies are used in military equipment and armament or for establishing and functioning of military organizational systems and their networks (command, control, and support), the use of information technologies is significant, obvious and increasing.

Comprehensive applications of information technologies and abilities of system and processes networking are so extensive that this caused a creation of a completely new, fifth domain of military activities – cyber space, which represents: "A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." (US Army Joint Staff, 2013, p.5). Within the information domain, cyber space is characterized by the application of different types of information technologies (analogous and digital electronic, opto-electronic and even quantum technologies). The information domain consists of physical, information (including logical), and cognitive dimensions or layers (U.S. Army Joint Staff, 2014). This means that within the complete cyberspace there are different factors and elements which perform activities and they represent the basis of the cyberspace infrastructure: people, hardware, software, environment, power, networks, payload, and policy (Rauscher, 2004). These elements can be put into three key sets that constitute cyberspace, including its part used by military organizations: people, processes and systems (Godwin, et al, 2014).

Vulnerability assessment and penetration testing in the military environment

Along with the already mentioned importance of information technologies for the operation of military organizational systems and their interconnectedness within cyberspace, cyber infrastructure is crucially important to all vital services, sustainable operations and restorations of cyberspace and organizations and systems that are using it to achieve the-

ir purpose (Godwin, et al 2014). The key factor for their safe operation is protection from threats (internal or external) across all the mentioned layers. This relates not only to military systems, whose basic function is national defense, but also to all governmental and private organizations as well as individuals. This is why violation of information security often simultaneously relates to different legally regulated forms of security (national defense, but also all types of crime, including terrorism and espionage). The circumstance that conflicts in cyberspace are based on discovery and exploitation of vulnerabilities and deficiencies makes their legal regulation significantly more complex. There are so many threats that entities in charge of defense of a system cannot even perceive their total number and scope. The existing threats are changing and evolving in time, along with the development of the immediate and wider environment. They are especially extensive in the field of information security, given the numbers and variety of technologies in modern global environment, as well as mutual connections between factors that influence all phases of the information system life cycle (Donohoe, 2012). Threats are directly connected to vulnerabilities and weaknesses of a system, whether they are known to its defenders or not. In the field of information security, there is a constant and endless race between attackers and defenders that consists of competing who will be the first to discover vulnerabilities or weaknesses of a system, across every layer of the information domain (physical, information and logical and cognitive levels). Causes for these vulnerabilities are numerous and can be found at all levels of creation, use and delayed effects of these technologies; they can be grouped in several general categories:

a. Due to growing requirements for resource optimization, military systems use the same or similar information technologies as civilian structures. These commercial off-the-shelf (COTS) technologies, whether proprietary or open source, are available to everyone, defenders and attackers alike.

b. A complex supply chain of information technologies and globalization make certain segments of these technologies so connected and intertwined that causes of vulnerabilities in them can be found even in technologies created specifically for military systems (Mattern, 2015).

c. Number and scope of information technologies that oftentimes are not harmonized with each other in all elements cause occurrence of new vulnerabilities that appear during interaction between these technologies.

d. General digitalization of everything and fast expansion of information technologies cause an increasing number of

information infrastructure parts or elements that influence this infrastructure to become subject to the existing vulnerabilities.

These vulnerabilities cause asymmetry of conflict in cyberspace. Since they are subject to (purposeful or accidental) revealing and exploitation by any attacker, the number of potential conflict participants grows rapidly, both attackers and defenders. The existence of vulnerabilities makes even the biggest systems subject to actions of small groups, even individuals. Today, there is a frequent situation where military forces of foreign governments can attack private companies in other countries, like in the case of Sony (Nakashima, 2014), or that the biggest countries can take legal and political measures against individuals as U.S. President Obama ordered in April 2015 (Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities) (Obama, 2015).The consequence of this is increasing the number of potential conflicting actors and extremely complex conflict environments.

What are vulnerabilities?

When causes of susceptibility to threats are considered, it is important to state what vulnerabilities are and how they occur. According to the National Information Assurance (IA) Glossary (Committee on National Security Systems, 2010), vulnerability is "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source". According to Herrmann (2007), whether accidental or intentional, vulnerability is a weakness that can occur in security requirements, system design, implementation, installation, operational procedures, configuration, and concurrent physical and personnel security controls, which makes this system susceptible to threats. In most general sense, in relation to the status of exposure to threats, vulnerability is absence of safeguard (Everetts, 2015).

Vulnerabilities lie in the basis of information security. According to the following conceptual equation, they are the basic risk factor in the field of information security:

$$Level\ of\ Risk = \frac{(Threats \times Vulnerabilities)}{Countermeasures} \times Impact \quad \text{(Everetts, 2015)}$$

This means that by discovery, removal or utilization of vulnerabilities, risk management can be universally influenced for the reduction of risks (prevention and mitigation of attacks), but also for the utilization of the existing risks of the adversary (for offensive activities, such as attacks or cyber exploitation). All these activities are achieved by influencing informa-

tion security, regardless of whether they are legally characterized as crime or armed conflict and regardless of whether they relate to defense or offense.

In defense, discovering vulnerabilities is the central part of risk assessment, involving analyses and evaluations which weaknesses and enemy activities may cause a negative influence on an organization and to what extent (Committee on National Security Systems, 2010, p.61). This activity is so significant that it represents a part of every Risk Management Framework. According to the recommendation of the National Institute for Standards and Technology (NIST), a vulnerability-oriented risk analysis should be a part of every risk management program (Cyber Intelligence Task Force, 2014), (NIST, 2012). Its goal is to maximally reduce the attack-surface model consisting of all possible layers of cyberspace and its infrastructure (U.S. Department of the Army, 2010). This leads to a conclusion that every discovery of the adversary's attack-surface enables a greater success in undertaking offensive cyber operations.

The goal of this analysis is to discover the existing vulnerabilities in one's own system, to describe them and give the technical specifications of the necessary steps for an attacker to exploit these vulnerabilities during an attack. This process is so important that it cannot be left out in any model of the information security risk management life cycle, where it is connected with other risk management processes. It must be repeated in regular intervals during a complete life cycle of a system. This is a universal case, whether a risk management model was defined by a generally accepted international (International Organization for Standardization, 2009), national (NIST, 2011) or proprietary enterprise (Committee of Sponsoring Organizations of the Treadway Commission, 2004), standard or framework.

Every vulnerability can lead to a situation where its exploitation is possible, accidental or purposeful. If conflicting sides use the same information technologies, characterized by the same vulnerabilities, discovery and technical specifications of necessary steps for exploiting vulnerabilities can be equally used for the prevention of adversary's attacks and for attacking the adversary (if the same vulnerability exists in the defended and the attacking system). This circumstance relates the skill of cyber warfare with the art of obtaining knowledge of vulnerabilities and weaknesses in information systems (and their corresponding infrastructure).

Vulnerability assessment and penetration testing

In the process of risk management assessment, in dealing with vulnerabilities, the process of vulnerability assessment should not be confused with penetration testing. Although these two concepts are similar and highly connected, they are different in their nature. The National Institute of Standards and Technology describes penetration testing as "a test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system" (NIST, 2014, p.B-7). According to the same source, vulnerability assessment (discovery and analysis) represents a systematic examination of an information system for the purpose of determining adequacy of security measures, determining deficiencies, and finding and undertaking security measures to eliminate influence of threats and reduce risks (National Institute for Standards and Technology, 2013). Therefore, penetration testing is a specific type of assessment of an information system (usually technically oriented), implemented for the purpose of determining the existence of vulnerabilities. Penetration testing is an imitation of an adversary's activity on one's own system for the purpose of pre-emptive defense. This is why penetration testing is the one procedure that makes vulnerability assessment common for both attack and defense. The development of the penetration testing methodology is connected to professional knowledge on technology and system organization and represents the application of the information technology body of knowledge in the military environment.

Military systems are specifically security oriented, since their purpose is defense of their own systems (by military means and methods) and disabling and destruction of enemy systems. In this military business, different areas of security are simultaneously planned, applied and analyzed so that vulnerability assessment and penetration testing, (that are especially characteristic for information security in contemporary organizations), are used in all other security-related areas, from physical to information security. Having in mind the already mentioned fact that in modern times all human activities depend on information technologies and cyberspace, as well as that the information area consists of wide infrastructure in a physical, information, logical and cognitive sense, it is clear that penetration testing can be undertaken for hardware, software, people and processes and it can relate to different types of security controls (physical, organizational, and technical) (NIST, 2013).

Penetration testing relates to finding vulnerabilities in proprietary or other systems, as well as to estimating a degree of resistance that infor-

mation and organization systems has against enemy activities in relation to the time necessary for breach of defense, necessary resources and skills (NIST, 2013). This universal defense/offense method applied by military and intelligence organizations is at the same time an indispensable element and a phase of every risk management process. It consists of various techniques and methods for finding vulnerabilities, and it is a part of other, broader activities, such as security monitoring, establishment of security configuration settings, establishment of policies, strategies and procedures for secure system use. Penetration testing implemented for the purpose of defense and offense does not differ much in the technology and technical approach applied, but exclusively in goals and intentions of penetration testing practitioners, within and limited to their goals and tasks. This is why training of individuals and teams for penetration testing does not have to be implemented separately for defense and offense. It is important to point out that vulnerability assessment represents the key area for collaboration of national military and intelligence organizations in cyberspace (Cyber Intelligence Task Force, 2014). This is why the use of these activities by state bodies and institutions is significant in respect of legal regulations, in both national and international laws, especially regarding the specific application of the IHL.

Education, training and legal regulation of vulnerability assessment and penetration testing

Knowledge necessary for the implementation of vulnerability assessment and penetration testing is primarily technical in its nature and requires high specialization and experience. This is why these activities (in the civilian environment) are often implemented by external providers (NIST, 2003). In practice, it is done by intelligence agencies and other organizations that do not perform attacks on military targets, that use results of external collaborators as a service, since such testing activities require human involvement, even if automatic methods by the application of specialized software or devices are used (NIST, 2003). However, in the military environment, these activities are used for the discovery of vulnerabilities in enemy military systems or for attacks on foreign targets. This sets limitations of legal nature, due to the provisions of the Law of Armed Conflict. Protocol Additional to the Geneva Conventions of 12 August 1949 states in Article 43 that "members of the armed forces of a Party to a conflict (other than Medical personnel and chaplains" (1125 UNTS 3, 1977, art. 43) are combatants who have the right to participate directly in hostilities. Howe-

ver, no international regulations strictly forbid civilians to take direct participation in hostilities. A group of experts in the field of international humanitarian law at the invitation of The NATO Cooperative Cyber Defence Centre of Excellence in Tallinn gave their expert opinion on participation of civilians in cyber warfare, where "Civilians are not prohibited from directly participating in cyber operations amounting to hostilities but forfeit their protection from attacks for such time as they so participate" (Schmitt, 2013, p.90).

However, according to various national laws and military rules of engagement and manuals, participation of civilians in hostilities is unlawful (for example in Canada, Côte d'Ivoire, Germany, Indonesia, Italy, Nigeria, Peru, Spain, United Kingdom, and other) (International Committee of the Red Cross, 2015). In some countries with common law tradition, such as the U.S, there are cases where in different stages of a case court decisions were made according to which participation of alien civilians in hostilities was treated as unlawful (McCarthy, 2007), because they were civilians who took part in hostilities, therefore, they were neither lawful combatants nor lawful civilians.

It is, nevertheless, necessary to point out that there is still no universal international consensus on this issue, since no treaty law nor customary law precisely define what represents direct participation in hostilities, as pointed out in the Pre-Trial Chamber of the International Criminal Court in the Case of the Prosecutor v. Bahar Idriss Abu Garda (ICC-02/05-02/09, 2010). Also, it is necessary to take into consideration the complexities of a situation where development of technology and its application in hostilities is an important factor of additional complexity of international legal regulations of conflicts in which civilians participate in one of possible ways (Schmitt, 2004). Even without this dominant factor today, the existing provisions and rules of International Humanitarian Law, some of which are more than a hundred years old, are imprecisely and unclearly defined because they were adopted through consensus of all international parties (states), which is an almost impossible task in practice due to their different interests and traditions.

The already mentioned legal reasons and requirements to achieve confidential military information secrecy in military organizations require that vulnerability assessment and penetration testing be done by members and groups from the military itself. To achieve this, it is necessary to systematically train members of the military who perform these activities. In doing this, there should be no compromises, because their training and qualifications are what key activities in cyber defense and warfare depend on. Besides requirements for top achievements, their training should be continuous, since search for vulnerabilities is a constant process that must

be improved and developed all the time. The focus during training should be put on education in relation to gaining awareness and training, since this activity is considered to be a key one within the Information Technology Security Learning Continuum for the creation of appropriate information technology security specialists and professionals (NIST, 2003; 1998). However, since these are top experts, no form of professional improvement and development should be neglected, such as advanced training and even research activities.

Need for research and development in vulnerability assessment and penetration testing

Research in the field of information security vulnerabilities and penetration testing is an especially important field, since there is the requirement that new solutions for system breach be constantly developed. Personnel must constantly be trained in new techniques and methods. This is why there must be a close collaboration between military organizations and academic research institutions, industrial research and development centers and small, private teams and even individuals. This means that asymmetry in information security for the purpose of conducting military conflicts does not reflect only in differences between enemies, but also in enlistment of collaborators. This asymmetry is enabled by high specializations in specific fields; particularly suitable for such applications are penetration testing of software systems, services and applications.

Every software contains vulnerabilities that are a consequence of errors in coding and lack of coordination in processes and interactions between different software technologies. According to McConnell, the industry average number of coding errors in 2004 was between 1-25 errors per 1000 lines of programming code and 0.1 error per 1000 lines of code in the highly efficient special development technique (2004, p.25).The same author states that in only a few known cases, primarily in the space shuttle technology, with the application of specific methods which slow down and significantly increase costs of the coding process, a success of zero errors in 500,000 lines of code was achieved (McConnell, 2004). However, history shows that even in such cases software errors go unnoticed by penetration testers, like in the case of explosion of ARIANE 5 rocket explosion in 1996 (Inquiry Board, 1996). Along with the development of new technologies, their application in complex combat systems grows. For example, the most complex multipurpose military aircraft in development, Lockheed-Martin F-35 Joint Strike Fighter, has over 24 million code lines so

far, mostly done in C and C++ languages, and their numbers continue to grow as new systems and requirements are added (Charette, 2012). In such a number of code lines, it is to be expected that there is a number of errors and lack of process coordination that might be used in the future for a cyber attack. Even before the initial exploitation of the aircraft, industrial espionage in cyberspace enabled penetration testing experts of a potential future enemy to find suitable exploits whose application might achieve kinetic consequences to combat systems in a potential future conflict (The Wall Street Journal, 2014).

Need for the formation of vulnerability assessment and penetration testing teams within military organizations

Once exploited vulnerability is easier to discover and through (ab)use it stops being suitable for a new application. It is also important to know where to look for defects and vulnerabilities, because there are differences in the number of coding defects in software written in different program languages (Ray, et al, 2014, pp.155-165). This is why attackers must be experienced and trained, because they are expected to quickly and clearly make an evaluation of a choice of vulnerability in specific situations. For example, in the report of Kaspersky company on breaches into information systems of many countries by the Equation group, there was discovered a systematic regularity on the application and hierarchy of choice of targeted systems vulnerability information in relation to their significance (Kaspersky Labs, 2015). This is why it is believed by experts that an attacker group most probably represents a unit of an intelligence agency of a technologically developed country. It is not likely that adversary vulnerability information will be used over a longer period of time. Most valuable are those vulnerabilities that are not discovered by anyone, except for attackers, in the moment of the attack. They are called zero-day vulnerabilities and are used to initiate zero-day attacks. Software or a method, a set of data, a sequence or an attack command which uses the zero-day vulnerability is called the zero-day exploit. The more software is widespread, the more interesting it is for different penetration testing teams that find new zero-day vulnerabilities. The world of penetration testing thus comes down to an eternal race between attackers, defenders and manufacturers who, for their own reasons, are all trying to discover as many vulnerabilities as possible and use them for attack or defense. Although all big softwa-

re companies pay independent researchers for information on zero-day vulnerabilities, the market for information about them is growing. It is joined by state agencies and specialized penetration testing and vulnerability assessment companies and teams which even have regular clients among agencies (Perlroth & Sanger, 2013). The most well-known are Vupen (Vupen Security, 2015), Revuln (Revuln, 2015) and Netragard (Netragard, 2015).

Even though such a collaboration model can successfully help attempts of information infrastructure protection and conducting offensive operations in cyberspace, it is not sufficient for all the needs at the national level. Within military forces, it is necessary to form groups and teams for vulnerability assessment and penetration testing that are made up of experienced and highly skilled individuals. An example of a successful organization in these activities which applies the methods and techniques described is Tailored Access Operations, a group within the National Security Agency (Aid, 2013). However, regardless of being formed as a part of a global military force or a small country army, vulnerability assessment and penetration testing organizations within armies must have their structural freedom and organizational independence from the rest of the army. Given the basic value that unites members of such teams, which is highly specialized knowledge and skills, the traditional vertical hierarchy makes their functioning and development harder and limits creativity. This is why such units are always more efficient if they follow an unconventional, problem solving-oriented organizational structure.

Conclusion

Vulnerability assessment and penetration testing are a central part of all defensive and offensive military activities in cyberspace. At the same time, they are a key part of a comprehensive process of risk management, without which compliance requirements of any information organization system cannot be achieved. Information security risk management represents organizational management of people, processes and systems. Vulnerability assessment and penetration testing are primarily oriented to information technologies and the way people interact with them. Even though these activities have the same focus, same technologies and processes, their goals are different but complementary. There are defects, flaws and weaknesses in every information system. Their nature varies widely and the number is always increasing. Information on vulnerabilities is the goal, both for the system's author and defenders and attackers and there is always a competition between these sides who will obtain the valuable

information first. Owning the same information on vulnerabilities enables the prevention of threats (external and internal), but at the same time it enables exploiting adversary's weaknesses. Due to this characteristic, vulnerability assessment and penetration testing are equally important for the risk management process, offensive and defensive military and intelligence operations in cyberspace. If, by a process of elimination, different activities in the mentioned fields of information security are removed, it is clear that its tasks cannot be achieved without vulnerability assessment and penetration testing. Their activities can be outsourced to organizations outside the military, but having in mind the confidentiality requirement and limitations set by International Humanitarian Law, it is necessary for units working on these activities to be a component of military organizations. Nevertheless, having in mind the need for specific knowledge and skills, and requirements for constant research, their organizations must be specific and set in a way so as not to be disturbed by the traditional military vertical organizational hierarchy.

References

Aid, M., 2013. *Inside the NSA's Ultra-Secret China Hacking Group.* [Internet]. Foreign Policy. Available at: http://foreignpolicy.com/2013/06/10/inside-the-nsas-ultra-secret-china-hacking-group. Accessed: 12 Apr. 2015.

Charette, R., 2012. *F-35 Program Continues to Struggle with Software*. [Internet] IEEE Spectrum: Technology, Engineering, and Science News. Available at: http://spectrum.ieee.org/riskfactor/aerospace/military/f35-program-continues-to-struggle-with-software. Accessed: 12 Apr. 2015.

Committee on National Security Systems, 2015. National Information Assurance (IA) Glossary, CNSS Instruction No. 4009 April 6, 2015. Ft Meade: National Security Agency.

Cyber Intelligence Task Force, 2016. *Strategic cyber intelligence*. [Internet] Intelligence and National Security Alliance. Available at: http://www.insaonline.org/i/d/a/b/StrategicCyberWP.aspx. Accessed: 17 Apr. 2015.

Donohoe, M., 2012. A discussion on Supply Chain Risk and Mitigation. [online lecture]. Enterprise Information Security and Risk Management (ESS15-03), Week 9: Supply Chain Risk Management – Mitigation. Information Resources Management College, National Defense University.

Enterprise Risk Management: Integrated Framework, Executive Summary, 2004. [ebook]. Committee of Sponsoring Organizations of the Treadway Commission Enterprise. Available at: http://www.coso.org/documents/coso_erm_executivesummary.pdf. Accessed: 18 Apr. 2015.

Everetts, R., 2015. Risk Management: Foundation. [online lecture]. Enterprise Information Security and Risk Management (ESS15-03), Week 1: Introduction and Overview. Information Resources Management College, National Defense University.

Godwin, J., Kulpin, A., Rauscher, K., and Yaschenko, V., 2014. *Critical Terminology Foundations 2*. EastWest Institute and the Information Security Institute of Moscow State University. [Internet]. Available at: http://www.ewi.info/idea/critical-terminology-foundations-2. Accessed: 17 Apr. 2015.

Herrmann, D.S., 2007. Complete guide to security and privacy metrics, Measuring regulatory compliance, operational resilience, and ROI. Boca Raton: CRC Press.

Inquiry Board, 1996. *ARIANE 5 Flight 501 Failure*. [Internet]. Available at: http://sunnyday.mit.edu/accidents/Ariane5accidentreport.html. Accessed: 17 Jan. 2016.

International Committee of the Red Cross, 2015. *Practice Relating to Rule 6. Civilians' Loss of Protection from Attack. Customary IHL Database*. [Internet]. Available at: https://www.icrc.org/customary-ihl/eng/docs/v2_rul_rule6. Accessed: 17 Feb. 2016.

International Organization for Standardization, 2009. ISO 31000: 2009. Available at: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en.

Kaspersky Labs, 2015. *Inside the EquationDrug espionage platform*. [Internet]. SecureList. Available at: http://securelist.com/blog/research/69203/inside-the-equationdrug-espionage-platform. Accessed: 22 Mar. 2016.

Mattern, R., 2015. Supply Chain Risk Management: Mitigation. [online lecture]. Enterprise Information Security and Risk Management (ESS15-03), Week 9: Supply Chain Risk Management: Mitigation. Information Resources Management College, National Defense University.

Mccarthy, A.C., 2007. *Military Judge Dismisses Commission Charges Against Omar Khadr*. [Internet]. National Review. Available at: http://www.nationalreview.com/article/221180/military-judge-dismisses-commission-charges-against-omar-khadr-andrew-c-mccarthy. Accessed: 12 Apr. 2016.

Mcconnell, S., 2004. *Code complete: A practical handbook of software construction*. Redmond: Microsoft Press.

Nakashima, E., 2014. *U.S. attributes cyberattack on Sony to North Korea*. [Internet]. Washington Post. Available at: http://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html. Accessed 17 Apr. 2016.

National Institute for Standards and Technology, 2003. Guide to Information Technology Security Services. U.S. Department of Commerce. Special Publication, pp.800-835.

National Institute for Standards and Technology, 1998. Information Technology Security Training Requirements: A Role- and Performance-Based Model. Gaithersburg, MD. U.S. Department of Commerce. Special Publication, 800-16.

National Institute for Standards and Technology, 2011. Managing Information Security Risk, Organization, Mission, and Information System View. Special Publication.800-39. Gaithersburg, MD.U.S. Department of Commerce.

National Institute for Standards and Technology, 2012. Guide for Conducting Risk Assessments. U.S. Department of Commerce. Special Publication 800-30, Revision 1. Gaithersburg, MD.U.S. Department of Commerce.

National Institute for Standards and Technology, 2013. *Security and Privacy Controls for Federal Information Systems and Organizations* [includes updates as of 01-22-2015]. Special Publication 800-53, Revision 4. Gaithersburg, MD. U.S. Department of Commerce.

Netragard, 2015. Available at: https://www.netragard.com.

Obama, B., 2015. Executive Order: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities. Available from: https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m. Accessed 1 Mar. 2016.

Perlroth, N., & Sanger, D.E., 2013. *Nations Buying as Hackers Sell Flaws in Computer Code*. [online] New York Times. Available at: http://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html. Accessed 11 Apr. 2016.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 1949. Geneva. 1125 UNTS 3.

Rauscher, K.F., 2004. Protecting communications infrastructure. *Bell Labs Tech. J.*, 9(2), pp.1-4.

Ray, B., Posnett, D., Filkov, V., & Devanbu, P., 2014. A large scale study of programming languages and code quality in Github. In: Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering. New York: ACM, pp.155-165.

Revuln, 2015. Available at: http://revuln.com.

Schmitt, M., 2004. Direct Participation in Hostilities and 21st Century Armed Conflict. In H. Fischer& et al Eds., Crisis Management and Humanitarian Protection: Festschrift fur Dieter Fleck. Berlin: BWV, pp.505-529.

Schmitt, M.N., 2013.*Tallin Manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press.

Situation in Darfur, Sudan, in the Case of the Prosecutor v. Bahar Idriss Abu Garda, 2010. February 8, ICC-02/05-02/09 (Pre-Trial Chamber I Decision on the Confirmation of Charges).

The Wall Street Journal, 2014. *China's Cyber-Theft Jet Fighter,* Available at: http://www.wsj.com/articles/chinas-cyber-theft-jet-fighter-1415838777. Accessed: 11 Apr. 2016.

U.S. Army Joint Staff, 2013. Cyberspace Operations3-12 (R). Joint Publication, pp.3-12.

US Army Joint Staff, 2014. Information Operations, 27 November 2012 Incorporating Change 1 20, pp.3-13

U.S. Department of the Army, 2010. *Cyberspace Operations Concept Capability Plan 2016-2028, TRADOC Pamphlet 525-7-8*. US Army Training and Doctrine Command (TRADOC).

Vupen Security, 2015. Available at: http://www.vupen.com/english.

ОЦЕНКА УЯЗВИМОСТИ И ТЕСТИРОВАНИЕ НА ВЗЛОМ В ВОЕННОМ И МЕЖДУНАРОДНОМ ГУМАНИТАРНОМ ПРАВЕ

Драган Д. Младенович
Вооруженные силы Республики Сербия, Генштаб, Управление телекоммуникаций и информатики (J-6), г. Белград, Республика Сербия

Резюме:

Оценка уязвимости и тестирование на взломвляются ключевой деятельностью управления информационной безопасностью и рисками киберобороны, а также разведки, проводимой военными организациями. Эти мероприятия имеют важное значение не только в контексте выполнения военных операций, но и в международном гуманитарном праве (МГП) и правоохранительных контекстах. Применение информационных технологий в военных и гражданских условиях увеличивает сложность в области управления рисками. Помимо информационной безопасности, военные организации должны проводить необходимые мероприятия в области кибероперации, как для защиты, так для нападения целей.

Они зависят от технологических знаний и навыков и реализуются конкретными подразделениями в рамках военных систем. Цель оценки уязвимости заключается воткрытии характера уязвимости, не анализируя, как они могут быть использованы приатаках. В то время как тестирование на проникновение использует эксплойт-вторженияво время атаки на системуи таким образом производит классификациютипа и степенириска уязвимости для системы.

478

Тем не менее, хотя они и представляют собой два различных вида деятельности с разнымицелями, их взаимодействие неразделимо, так как они взаимосвязаны и дополняют друг друга. Общей чертой данных мероприятий является развитие знаний и навыков, основанных на тех же технологиях, и они одинаково важны как для управления рисками в военных операциях в киберпространстве, так и в области обороны, разведки и международного гуманитарного права.

Ключевые слова: оценка уязвимости, тестирование на проникновение, кибератаки, Международное гуманитарное право.

ПРОЦЕНА РАЊИВОСТИ И ТЕСТИРАЊЕ ОТПОРНОСТИ НА УПАДЕ У СИСТЕМ У ВОЈНОМ И КОНТЕКСТУ МЕЂУНАРОДНОГ ХУМАНИТАРНОГ ПРАВА

Драган Д. Младеновић
Војска Србије, Генералштаб, Управа за телекомуникације и информатику (Ј-6), Београд, Република Србија

Сажетак:

Процена рањивости и тестирање отпорности на упаде у систем су кључне активности управљања ризиком у информационој безбедности, сајбер одбрани и обавештајном раду војних организација. Ове активности су значајне у контексту извођења војних операција, али и у контексту Међународног хуманитарног права (IHL) и спровођења закона. Примена информационих технологија у војном и цивилном окружењу повећава комплексност у области управљања ризиком. Поред информационе безбедности, војне организације имају задатак да предузму неопходне активности у области сајбер операција, за сврхе одбране и напада. Они зависе од знања и вештина заснованих на технологији и имплементирају их специфичне организације у оквиру војних система. Процена рањивости за циљ има откривање природе рањивости, без разматрања како се оне могу користити за напад, док тестирање отпорности на упаде у систем користи експлоите за упаде у системе и тако процењује врсту и степен ризика који ове рањивости представљају за систем. Међутим, чак и ако представљају две различите активности, са различитим крајњим циљевима, они су комплементарни и међузависни. Пошто је њихова заједничка одлика развој знања и вештина заснованих на истим технологијама, они су од подједнаке важности за управљање ризиком, војне операције у сајбер про-