A review of the challenges of the crisis management during the cyber attacks

Abdullah Oudah Alasmari

University of Newcastle, Australia

Abstract

This brief exploratory review was aimed at understanding the types of challenges in crisis management arising from cyber attacks. A brief survey of literature was done using Google Scholar as the search engine. The 34 usable works were discussed under appropriate cyber security contexts and dimensions. The challenges faced at individual user levels like online transactions, by businesses and other organisations, nations and their cooperatives like NATO were discussed in the contexts of minor and major cyber attacks to cyber warfare. The review demonstrated that solutions to the challenges are never perfect as the attackers are always one up even against the best protection systems devised.

Keywords: Crisis Management, Cyber Attacks, Challenges, Review

Background

A PwC report (PwC, 2019) notes that all cyber attacks on any organisation are facing increasingly complex types of cyber attacks over the years. These attacks cause immense damage in terms of economic, operational and reputational losses. Such attacks may be difficult to quantify. Leaders of organisations are always concerned about the acceptable levels of risks when cyber attacks happen. What types and levels of risks are acceptable is the first challenge for any organisation. These may vary widely. PwC reports that 65% of CEOs experienced at least one cyber attack in the last three years and 40% of them expect another one in the next three years. For 57% of the CEOs, their organisations are susceptible to such attacks any time.

The first step of crisis management is being crisis ready. Some characteristics of organisations which are ready for crisis ready for cyber attacks are listed in the same PwC report. These are: proactive identification of current and potential cyber threats, tools and technologies to manage crisis are ready and understood at all levels, the organisation has a quick response culture with the required empowerment at various levels, continuous improvement in crisis capabilities, training, rehearsing and exercising on crisis at the required levels and well-defined response priorities.

Another report by Deloitte (Deloitte, 2016) also discusses readiness, response and recovery as the three strategies of cyber security management. The challenge here is that no organisation can achieve total cyber security. An estimated three cyber attacks occur every minute. Not all succeed; probability of any of them becoming serious, is high. This is where the challenge of creating a proper cyber security management system becomes important. Coordinating the response and recovery measures when an attack occurs, is also a challenge.

According to Utreja (2018), multiple possibilities of cyber attacks (types and levels) pose the greatest challenge as it is almost impossible to be prevent new types of attacks evolving every time.

The aim of this brief exploratory review is to understand the types of challenges of crisis management when an attack occurs in diverse contexts and dimensions.

Method

This is not meant to be an exhaustive, but a short qualitative review of explorative nature. Published works related to the topic of review were identified from Google Scholar using appropriate search terms in both (any time frame and for the period from 2015 for recent works). The search yielded 34 usable papers. These papers were divided into subsections for discussions below.

Review

The nature of cyber security challenges

The challenges of cyber war consist of many specific characteristics, as was described by Cimbala (2011). Cyberwar has a distinct characteristic from the point of view of deterrence. There can be obvious overlaps in the real world situation. Cyber deterrence includes both uncertainties and complexities of various types and levels. Generally the identity of the attackers is obscure. The attacks can be initiated from outside or within the territory and frequently are mediated by third parties with or without their complicity or knowledge. It is possible to continue to attack repeatedly and almost indefinitely by skilled attackers, even if the defenders are alert.

Cyber attacks are increasingly becoming sophisticated and more frequent, forcing organisations to be proactive, but insufficiently, according to Kulikova, Heil, van den Berg, and Pieters (2012), who proposed a decision support system for security information system disclosure. According to Vande Putte and Verhelst (2014), huge challenge of cyber security management is due to the continuously changing nature and increasing sophistication of cyber threats. These two have increasing effect on their impacts. Cyber security management is further complicated by the society and its economy being increasingly dependent on information and communication technologies.

Uncertainties and risks of cyber threats in the globalised modern business scenario needs to be managed by modifying traditional risk analysis to build business resilience. This topic was elaborated by Crovini, Ossola, and Marchini (2018).

Citing the examples of the first major attack via the Internet of Things on a DynCorp server in the United States hacked through video surveillance cameras in 2016 and the first attacks driven by artificial intelligence and increasing evidence of collusion between state intelligence services and organized crime networks, Shea (2017) pointed out that the security agencies are unable to catch up with the speed and global impact of such attacks.

Infrastructure security challenges

One of the most vulnerable points of cyber attack is smart grids of power supply. Cyber attacks on the computerised control systems may disable the power supply totally, can block power distribution and trigger explosions in power plants. The challenge in this respect arises from the vast geographical area and thousands of consumers at the other end. These challenges were discussed by Line, Tøndel, and Jaatun (2011). Same types of challenges were identified in the case of European smart grids by Pearson (2011).

Threats and disruptions of physical infrastructure can lead to failure of cyber infrastructure also. Organising and managing massive amount of critical infrastructure data are challenging due to their geographical disparity. Kopylec, D'Amico, and Goodall (2007) developed a system, Cascade, to evaluate these effects using Actor-Network theory. Visual depiction of infrastructure data has been facilitated in this system, which makes planning disaster management and crisis response activities.

Challenges of cyber warfare

The possibility of deterring cyber attacks on multiple installations and sites of US forces and that of its allies is a major challenge for USA. In this respect, Kugler (2009) pointed out that USA currently has no cyber deterrence strategy against such threats. It may not be possible to deter all cyber attacks, but if major and most dangerous attacks could be prevented, it is an achievement. Globalisation has increased the vulnerability of organisations all over the world to cyber attacks. Political issues with Latin American countries, Middle Eastern countries, Russia, Afghanistan, trade wars with countries like China and increasing threats of terrorism are some factors contributing to challenges of cyber attacks on massive scales, for which USA and most other countries are not prepared for. Identities of many cyber attackers are not readily obtained. Some of them may have nee sponsored by hostile governments. On the other hand, some attackers may make their identity known for political and strategic gains. There had been many failures of US deterrence strategies in the past. So, deterrence theory does not hold good any more. USA needs to find other methods of cyber attack crisis management.

Internet, cloud computing, social media networks, and mobile phones have increased the challenges of cyber security in the modern times. Multidimensional and ambiguous nature of cyber attacks and therefore security frames and the cooperative efforts by Nordic countries were discussed by many authors in the book (Rantapelkonen & Salminen, 2013).

The challenge of cyber warfare lies in its being a potent tool which can be used in political conflicts, espionage, and propaganda. It is difficult to detect in advance and is often detected only after significant damage has been done. Perpetrators and victims usually act as if nothing has happened and the evidence erases itself. Pointing out to these challenges, Goel (2011) noted that there is intense competition among leading countries like USA, Russia and China to develop offensive cyber attack capabilities.

Although both USA and China are aware of each other’s cyber attack capabilities and the relative first strike advantages, both fail to consider the risks involved in connecting military advantages of cyber attacks with strategic hazards (Gompert & Libicki, 2014). A cyber warfare between them can trigger a military war or a war between them would consist of both cyber and military wars. There are many hotspots of political instability in which the two are against each other. In addition, intense trade war has also started recently.

Development of sufficient analytical, warning and responding capabilities of institutions charged with cyber protection can be a challenge, as a report of General Accounting Office (GAO) on US National Infrastructure Protection Centre (NIPC) (Dacey, 2001) shows.

In his article, Geers (2009) observed a certain level of disorder can be achieved in the real world even by cyber attacks of minor nature. Recent cyber attacks in Israel and Estonia are given as evidence. The law enforcement and counterintelligence are challenged to find answers to these and more serious types of cyber attacks in future.

In cyber warfare type attacks, the culprits are diverse and unknown and physical distance is not a factor. Offense is cheaper than defence because internet was designed for ease of use rather than for security. These characteristics of cyber attacks/wars were noted by Nye (2011). Some other aspects of cyber attacks are: the potential utility of weapons for both tactical and strategic purposes, the possibilities of scenarios related to the first- and second-users and unintended consequences and cascading effects of a new and poorly understood technology. Civilian use and military use of cyber space are different. In most nations, civilian control over military exists to prevent arbitrary attacks based on mere military perceptions. Most of the Internet and its infrastructure in most countries are owned and operated by private sector and the government has only very limited regulatory leverage. Thus, private sector becomes a constraint on cyber policy. It has been recognised that there is always a high level of cyber risk. Hence, the strategy should have in-built redundancy and resilience after attack. Internet service providers do not have economic incentive to provide cyber security beyond a point. Competitive pricing also restricts provision of security beyond a level. On the other hand, disclosure of cyber intrusions into their systems may undermine public confidence. So, they have an incentive in not disclosing cyber attacks or even admitting an attack has occurred and they tend to blame it on system failures. Hiding such information leads to lack of reliable data on which adequate protection can be formulated. This reduces the level of preparedness against cyber attacks. Differences of perspectives and mutual mistrust governs public-private partnerships. Inter-governmental cooperation and international standards on internet and cyber uses are some areas complete success has not been achieved.

The collective crisis management capabilities of EU to detect and making sense of crisis have improved, but not that of decision making. The capabilities of detection, sense-making, decision-making, coordination, meaning-making, communication, and accountability were more sector-oriented, and no cross-sectoral capability was noted. Most of these are confined to European Commission and percolated to other institutions of EU. Improvements in some tools for more analytical levels have been noted Backman and Rhinard (2018).

The challenges underlying cyber security preparedness of nations, organisations and local agencies were discussed by Pfeifer (2018). He pointed out that cyber attacks are used to steal intellectual property worth huge amounts, to influence elections, to manipulate news and to damage critical infrastructure. Cyberattacks are confined to technology problems to be handled by smart computer network technicians, who can discover these attacks and develop mitigating measures. On the top of such technical dimensions, targeted cyberattacks on critical infrastructure also cause denial of services. They also cause heavy damage and loss of life in the physical world.

Security challenges of online business

The challenges of protecting the large scale online transactions in India from cyber attacks were discussed by Tonge, Kasture, and Chaudhari (2013). Checklist-based security systems are insufficient. Internet privacy is low in India, adding to the challenge. Training people concerned with cyber security and making the public aware of the issues and how to protect themselves are two major challenges in India. Two general categories of cyber threats have been identified: actions aimed at and intended to damage or destroy cyber systems, cyber attacks and actions exploiting the cyberin frastructure for unlawful or harmful purposes without damaging or compromising that infrastructure, cyber exploitation. Some of these may not impact immediately and some of them may last long time. Activities included in cyber exploitation are: using the

cyber devices and tools to steal, to recruit and train terrorists, commit fraud, to convey controversial messages like political and hate speech, to violate copyright and other rules limiting distribution of information, and to sell banned materials.

Security challenges of e-learning systems

Security of e-learning systems has a unique challenge as these systems are accessed and managed via the Internet by thousands of users over hundreds of networks. The internet is prone to security threats like unauthorised access, accessing sensitive information, hacking, altering data and configurations, cracking and enabling academic misconducts. Therefore, academic institutions offering e-learning also need to implement appropriate cyber security management systems. A case study example of a IT management programme in a small university was presented by Ramim and Levy (2006) to illustrate these points. The insider cyber attack stopped all academic activities related to e-learning system of the university.

Communications issues of cyber security challenges

Lack of functioning of communication structures to act against disasters for repair and recovery has been pointed out as a major challenge by many researchers and a variety of approaches have been proposed. Reengineering system of systems (Waller & Craddock, 2011), crisis communication management on the internet (Alfonso & Suzanne, 2008), strategic intelligence management (Akhgar & Yates, 2013), resilient networks to operate under crises (Goel, Belardo, & Iwan, 2004) and emerging communication infrastructures (Asplund, Nadjm-Tehrani, & Sigholm, 2008). Decentralised communication architecture for secure data communication system between various agencies for crisis management was proposed by Rajamaki, Rathod, and Holmstrom (2013).

Public management issues of cyber security challenges

Uncertainty, urgency and threat are the three challenges of crisis situations in public management. The European tools have focused on the administrative capabilities for trans-boundary crises for involving its member countries. These points were noted by Blondin and Boin (2018). Cyber threat was conceptualised as socio-technical threat by the contributors of the book (Hills, 2016) due to the human-computer interaction inherent in it. Therefore, they argue for leveraging socio-technical capabilities to counter such threats by prevention and response activities.

Cyber threats often originate from transboundary spaces, noted Boin (2018). National governments are surprised by the impact of such threats and discover that existing crisis management arrangements are insufficient. There are political and administrative challenges when transboundary crises happen. Arrangements and processes that work reasonably well crises within national boundaries are unlikely to work when transboundary crises happen. If governments are unable to take effective actions, the images of political leaders and public institutions are damaged. Transboundary crises may have multiple domains, multiple actors, multiple types of impacts, may strike after a dormant period, hard to find the course and conflicting responsibilities among coordinating and centralising mechanisms. The main challenge is that the threat crosses the sovereign border of the country. Governments are reluctant to give decision making power to any other agencies even in the case of international cooperative agencies like EU.

In an analysis of management of various types of crises, Kessel and Masella (2016) discussed IT related issues also. Efficiencies can be seriously affected by IT problems and outages. The problems will be more severe in the case of small companies without established infrastructure. Plans addressing data privacy and IT security, increased use of cloud computing and mobile platforms and usage of personal devices by employees in the workplace are all dimensions which increase such threats, for which complete solutions may be difficult.

Big data security challenges

Challenges involved in big data security were examined by Benjelloun and Lahcen (2019). Big Data security consists of three aspects. They are, information security, security monitoring and data security. Security of big data is mainly concerned with a real-time monitoring to detect vulnerabilities, security threats and abnormal behaviours. There should be a provision for a granular role-based access control. A robust protection of confidential information is necessary. The security system should be capable of generating security performance indicators. The system should also support a rapid decision-making component when a breach of security incident arises. By its very nature, it is difficult to protect all data. If security layers are added increasingly, the system slows down and dynamic analysis of data is affected. Access control and data protection becomes two big challenges in the case of big data security. The difficulty of data classification and handling management of data dispersed in different sources also makes big data more vulnerable to cyber attacks. High investment requirement, use of multiple clouds for storage and transfer of data and world-wide distribution of the data are additional security issues.

Conclusions

Challenges of many types exist in the diverse contexts and dimensions of cyber security scenarios. Although some possible solutions have emerged, achieving perfection will remain a dream as attackers are always one up on the abilities of the security systems anywhere in the world.

References

Akhgar, B., & Yates, S. (Eds.). (2013). *Strategic Intelligence Management.* Butterworth-Heinemann. doi:10.1016/C2012-0-06121-2

Alfonso, G.-H., & Suzanne, S. (2008). Crisis communications management on the web: how internet-based technologies are changing the way public relations professionals handle business crises. *Journal of Contingencies and Crisis Management, 16*(3), 143-153. doi:10.1111/j.1468-5973.2008.00543.x

Asplund, M., Nadjm-Tehrani, S., & Sigholm, J. (2008). Emerging information infrastructures: Cooperation in disasters. In R. Setola, & S. Geretshuber (Ed.), *International Workshop on Critical Information Infrastructures Security, CRITIS 2008. Lecture Notes in Computer Science, vol 5508*, pp. 258-270. Springer, Berlin, Heidelberg. doi:10.1007/978-3-642-03552-4_23

Bachmann, S. (2012). Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats–mapping the new frontier of global risk and security management. *Amicus Curiae*(88). Retrieved January 2019, from https://sas-space.sas.ac.uk/4562/1/1671-2132-1-SM.pdf

Backman, S., & Rhinard, M. (2018). The European Union's capacities for managing crises. *Journal of contingencies and crisis management, 26*(2), 261-271. doi:10.1111/1468-5973.12190

Benjelloun, F.-Z., & Lahcen, A. A. (2019). Big data security: Challenges, recommendations and solutions. In *Web Services: Concepts, Methodologies, Tools, and Applications* (pp. 25-38). IGI Global. doi:10.4018/978-1-5225-7501-6.ch003

Blondin, D., & Boin, A. (2018). Managing Crises in Europe: A Public Management Perspective. In E. Ongaro, & S. Van Thiel (Eds.), *The Palgrave Handbook of Public Administration and Management in Europe* (pp. 459-474). Palgrave Macmillan, London. doi:10.1057/978-1-137-55269-3_24

Boin, A. (2018). The Transboundary Crisis: Why we are unprepared and the road ahead. *Journal of Contingencies and Crisis Management*, 1-6. doi:10.1111/1468-5973.12241

Cimbala, S. J. (2011). Nuclear Crisis Management and "Cyberwar" Phishing for Trouble? *Strategic studies quarterly, 5*(1), 117-131. Retrieved February 2, 2019, from https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Cimbala.pdf

Crovini, C., Ossola, G., & Marchini, P. L. (2018). Cyber Risk. The New Enemy for Risk Management in the Age of Globalisation. *Management Control*(2 (Suppl)), 135-155. doi:10.3280/MACO2018-SU2007

Dacey, R. F. (2001). *Critical infrastructure protection: Significant challenges in developing analysis, warning, and response capabilities.* General Accounting Office. Retrieved February 2, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a394175.pdf

Deloitte. (2016). *Cyber Crisis Management: Readiness, response, and recovery.* Deloitte. Retrieved January 16, 2019, from https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Risk/gx-cm-cyber-pov.pdf

Geers, K. (2009). The cyber threat to national critical infrastructures: Beyond theory. *Information Security Journal: A Global Perspective, 18*(1), 1-7. doi:10.1080/19393550802676097

Goel, S. (2011). Cyberwarfare: connecting the dots in cyber intelligence. *Communications of the ACM, 54*(8), 132-140. doi:10.1145/1978542.1978569

Goel, S., Belardo, S., & Iwan, L. (2004). A resilient network that can operate under duress: To support communication between government agencies during crisis situations. *Proceedings of the 37th Annual Hawaii International Conference on System Sciences, 5-8 January 2004, Big Island, HI, USA* (p. 11 pp). IEEE. doi:10.1109/HICSS.2004.1265312

Gompert, D. C., & Libicki, M. (2014). Cyber warfare and Sino-American crisis instability. *Survival, 56*(4), 7-22. doi:10.1080/00396338.2014.941543

Hills, M. (2016). *Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection, Prevention and Response.* Nova Science

Publishers. Retrieved February 3, 2019, from http://nectar.northampton.ac.uk/8681/1/Hills20168681.pdf

Kessel, M., & Masella, R. (2016). Preparing for crises. *Nature biotechnology, 34*(2), 133-136. Retrieved February 3, 2019, from https://www.nature.com/articles/nbt.3475.pdf?origin=ppub

Kopylec, J., D'Amico, A., & Goodall, J. (2007). Visualizing cascading failures in critical cyber infrastructures. In E. Goetz, & S. Shenoi (Ed.), *Critical Infrastructure Protection, ICCIP 2007, IFIP International Federation for Information Processing. 253*, pp. 351-364. Springer, Boston, MA. doi:10.1007/978-0-387-75462-8_25

Kugler, R. L. (2009). Deterrence of cyber attacks. In *Cyberpower and national security* (p. 26 pp). Retrieved February 2, 2019, from https://s3.amazonaws.com/academia.edu.documents/39598215/Cyberpower-I-Chap-13.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1549091711&Signature=R5cKNRE8pKhqZdM424JkUfmAfuI%3D&response-content-disposition=inline%3B%20filename%3DCyberpower_I_Chap_13.pdf

Kulikova, O., Heil, R., van den Berg, J., & Pieters, W. (2012). Cyber Crisis Management: A decision-support framework for disclosing security incident information. *International Conference on Cyber Security (CyberSecurity), 14-16 December 2012, Washington, DC, USA* (pp. 103-112). IEEE. doi:10.1109/CyberSecurity.2012.20

Line, M. B., Tøndel, I. A., & Jaatun, M. G. (2011). Cyber security challenges in Smart Grids. *2nd IEEE PES International Conference and Exhibition on Grid Technologies (ISGT Europe), 5-7 December 2011, Manchester, UK* (pp. 1-8). IEEE. doi:10.1109/ISGTEurope.2011.6162695

Nye, J. S. (2011). Nuclear lessons for cyber security? *Strategic Studies Quarterly, 5*(4), 18-38. Retrieved February 3, 2019, from https://apps.dtic.mil/dtic/tr/fulltext/u2/a553620.pdf

Pearson, I. L. (2011). Smart grid cyber security for Europe. *Energy Policy, 39*(9), 5211-5218. doi:10.1016/j.enpol.2011.05.043

Pfeifer, J. W. (2018). Preparing for Cyber Incidents with Physical Effects. *The Cyber Defence Review, 3*(1), 27-35. Retrieved January 16, 2019, from https://www.hks.harvard.edu/sites/default/files/centers/research-initiatives/crisisleadership/files/Pfeifer_Cyber_CDR_V3N1_SPRG2018.pdf

PwC. (2019). *Cyber crisis management: Prepare, respond, recover services.* Retrieved February 2, 2019, from PwC UK: https://www.pwc.co.uk/issues/cyber-security-data-privacy/services/crisis-management.html

Rajamaki, J., Rathod, P., & Holmstrom, J. (2013). Decentralized fully redundant cyber secure governmental communications concept. *European Intelligence and Security Informatics Conference (EISIC), 12-14 August, 2013, Uppsala* (pp. 176-181). IEEE. doi:10.1109/EISIC.2013.39

Ramim, M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology (JCIT), 8*(4), 24-34. doi:10.4018/jcit.2006100103

Rantapelkonen, J., & Salminen, M. (Eds.). (2013). *The fog of cyber defence* (Series 2, Article collection 10 ed.). National Defense University. Retrieved February 2, 2019, from http://www.doria.fi/bitstream/handle/10024/88689/The%20Fog%20of%20Cyber%20Defence%20NDU%202013.pdf

Shea, J. (2017). How is NATO Meeting the Challenge of Cyberspace. *Prism, a Journal of the Center for Complex Operations, 7*(2), 18-29. Retrieved February 3, 2019, from https://apps.dtic.mil/docs/citations/AD1044679

Tonge, A. M., Kasture, S. S., & Chaudhari, S. R. (2013). Cyber security: challenges for society-literature review. *IOSR Journal of Computer Engineering, 2*(12), 67-75. Retrieved February 2, 2019, from https://s3.amazonaws.com/academia.edu.documents/51758486/K01226775.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1549095220&Signature=0Sz9R7jlwaTVa7DVpBuQw0%2B2xmI%3D&response-content-disposition=inline%3B%20filename%3DCyber_security_challenges_for_soci

Utreja, S. (2018). *Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism.* Indian Computer Emergency Response Team(CERT-In). Retrieved January 16, 2019

Vande Putte, D., & Verhelst, M. (2014). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers? *Journal of business continuity & emergency planning, 7*(2), 126-137. Retrieved February 3, 2019, from https://www.henrystewartpublications.com/sites/default/files/Vande%20Putte%20and%20Verhelst.pdf

Waller, A., & Craddock, R. (2011). Managing runtime re-engineering of a system-of-systems for cyber security. *6th International Conference on System of Systems Engineering (SoSE), 27-30 June 2011, Albuquerque, NM, USA* (pp. 13-18). IEEE. doi:10.1109/SYSOSE.2011.5966566