Framework for the Development of Computer Emergency Response Team in Pakistan

Haleemah Zia, Rabeea Imran, Rahat Masood, Muhammad Awais Shibli
Department of Computing, National University of Sciences and Technology, Islamabad, 44000 Pakistan
Email: {fhaleemah.zia, 14msisrimran, rahat.masood, awais.shiblig}@seecs.edu.pk

Abstract

The current dynamic development in the field of Information and Communication Technologies (ICT) has posed various threats to critical infrastructure of the government and private sectors across the world. To mitigate the occurrence of cyberattacks, there is a need for coordinated and centralized response from the state. Pakistan, due to several factors (such as its nukes, strategic location and prevailing terrorism) is in dire need of a national Computer Emergency Response Team (CERT) to tackle the issue at first hand. In this paper, we have discussed Pakistan's major cybersecurity issues and highlighted the importance of CERT in tackling them. We propose a high level strategy for developing CERT for Pakistan which will work at national level. The framework is divided into six major steps which range from awareness to professional development.

Keywords: Cybersecurity, Framework, CERT

Introduction

The current dynamic development in the field of Information and Communication Technologies (ICT) has created global connectivity through cyberspace. Reliance on complex and constantly evolving technology constitutes critical infrastructure of government and private sectors of any country (Haller, Merrell, Butkovic, & Willke, 2010). Like other nations, Pakistan is also progressing in the IT world. In-fact, IT is one of the most flourishing sectors of Pakistan with a potential to deliver outstanding results. Academic institutions are offering degree programs and producing young graduates equipped with latest knowledge and skills in IT. Such widespread use of technology has made enormous amount of confidential data available across the network.

In today's world, penetration of IT in business has elevated concerns over the security of critical as-sets. Network systems are now suffering from various threats and malware infection. Government and private sectors are confronted with uncertainty associated with cyberspace and there is a need to counter the situation effectively so as to mitigate financial loss, sustain the organization's standing in the sector and prevent loss of life (Haller et al., 2010).

Managing cybersecurity through a national strategy is the common need of all nations in the 21st century. Creating security awareness among users is one way to solve the issue; however there is a need to introduce a centralized and coordinated re-porting and response mechanism in order to mitigate cyberattacks effectively and efficiently. The general approach is to identify the attack, analyse, evaluate and mitigate its effects, document the security assessment and generate a global view of network security. To implement these strategies, Computer Emergency Response Teams have been developed in some major countries of the world. The two terms, "Computer Security Incident Response Team (CSIRTs)" and "Computer Emergency Response Teams", al-though slightly different from each other (Kabay, 2005), are often used interchangeably.

http://dx.doi.org/10.24949njes.v10i2.508

Few of the world's National level CERTs, such as those operating in Australia, India are Malaysia are members of Asia Pacific CERT (APCERT) (Member Teams: About APCERT / APCERT, n.d.) while CERT of Pittsburgh (The CERT Division — SEI— CMU, n.d.), United States (US-CERT:About Us, n.d.), United Kingdom (CERT UK :What We Do, n.d.) are operating separately at national level. The general services offered by these CERTs include incident handling, incident response, disaster recovery, penetration testing, data recovery, policy development etc.

Cybersecurity is inarguably vital for any state in order to maintain its standing in the constantly evolving world of IT. The Stuxnet, Flame and Red October from the past are a wakeup call for all nations. Pakistan holds special interest for foreign world because of its strategic location and nuclear assets. The issue becomes even more severe due to the fact that the country has not yet been able to formulate a cybersecurity law and if some progress is achieved, its implementation remains a challenge.

In this paper, we propose a basic framework for developing Computer Emergency Response Team for Pakistan (we call it PKCERT (Khan., 2013)), which will work at national level. We present some basic guidelines for the overall process. Observing how Computer Emergency Response teams have been formed around the world and evolved over time, the framework is a set of basic stages from which PKCERT would eventually evolve. The rest of the paper is organized as follows: Section 2 discusses related work; Section 3 highlights some key issues in Pakistan for which PKCERT would be helpful; Section 4 introduces the proposed framework and detailed steps for an operational CERT in Pakistan; Section 5 discusses how PKCERT would respond to the issues mentioned earlier; Section 6 concludes the paper and proposes direction for future work.

Related Work

Like all other countries, cybercrime in Pakistan is growing at a fairly fast pace and the laws addressing cybercrimes are still in the pipeline waiting to be implemented. There

are different forms of cybercrime in Pakistan, mainly involving cyberstalking, unauthorized access to computer systems, website hack-ing, theft of information, malware attacks, illegal interception of telecommunication, electronic funds transfer fraud and electronic terrorism (Homeland

Security: About the National Cybersecurity & Communications Integration Center, n.d.). In an attempt to counter these and others, Pakistan's government has taken various steps from time to time. In 2008, "Prevention of Electronic Crime Ordinance" was promulgated. The ordinance gave FIA (Federal Investigation Agency) exclusive rights to inspect and charge cases against cybercrimes (Cyber Crime Law Pakistan, n.d.). In September 2013, The Senate Committee on Defence and Defence Production, in collaboration with PISA (Pakistan Information and security Association) held a seminar in Islamabad on the first ever cybersecurity strategy. A seven point action plan was proposed to counter internal and external cyberattacks. This action plan called for the development of PKCERT; Pakistan's first ever Computer Emergency Response Team (Khan, 2013).

On 16th April 2015, the Government has introduced "The Prevention of Electronic Crimes Bill". It lays down punishments for various crimes such as illegal access of information systems, cyberterrorism, electronic forgery, identity theft and so on.

Currently different teams are operating in Pakistan; one is PakCERT (PakCERT :: Pakistan Computer Emergency Response Team, n.d.) and another one is National Response Center for Cyber Crimes (NR3C). They are providing services such as security assessment, penetration testing, and audits for ISO compliance, security policies framework, on-site training and forensic investigation. PakCERTs website lists defacement statistics from January 1999 to Au-gust 2008 (PakCERT :: Pakistan Computer Emergency Response Team, n.d.). NR3C works under the FIA with a mission to assist Law Enforcement Agencies in Pakistan (National Response Centre for Cyber Crime, n.d.). For effective response, NR3C is divided into divisions responsible for digital forensics, provision of incident response support, imparting training and workshops for public awareness and liaising with international CERT. Another group, NUST CSIRT, is a government sponsored entity working in collaboration with Military College of Signals (Military College of Signals, n.d.). Their website is active and displays latest threats and vulnerability database. This team also hosts training and awareness sessions (NUST-CSIRT., n.d.).

All the efforts mentioned above are commend-able and praiseworthy. However, there remains a need for a national level CERT in Pakistan which works under the direct authority of the government. We have researched the working of various national CERTs/CSIRTs across the world. The remaining part of this section highlights major findings.

The first CERT was developed at Pittsburgh in November 1998 in response to the Morris Worm at-tack. The team is now a registered trademark of Carnegie Mellon University (CMU). Presently, the government level CERT in US is US-CERT, which works as an umbrella organization of The National Cybersecurity and Communications Integration Center (NCCIC). The latter itself is working under the Department of Homeland Security (DHS) (Najam, 2014). In UK, a team was developed in March 2014 in response to the National Cyber Security Strategy. Officially working as CERT-UK (CERT UK Useful Documents and Links Comments, n.d.) now, their key responsibilities include national cybersecurity incident management, support of critical infrastructure and spreading awareness. They are working in collaboration with government departments, industry partners, organizational computer emergency response teams and other national CERTs to enhance understanding of cyber threats. CERT Australia provides incident response services, malware and log file analysis and keeps in touch with international partners to seek assistance on latest threats and vulnerabilities (Our Services — CERT Australia, n.d.). It believes in fostering ties with international partners to actively mitigate cyberattacks. The team actively identifies the attack controllers, reaches out to inter-national partners to take down the attack traffic and later on gives advice and consultation.

Studies (Cyber Security in Estonia, n.d.), (Tracking GhostNet: Investigating a Cyber Espionage Network, n.d.), (CERT Estonia, n.d.) reveal how different CERTs around the world have helped in mitigating the effects of cyberattacks at various points in time. Between April and May 2007, public and private sectors of Estonia suffered website defacement and coordinated DDOS attack (Cyber Security in Estonia, n.d.). Government of Estonia accused Russia for commencing the attack. How-ever, no solid evidence was found when the matter was investigated. It was because of the Estonia's established CERT that they were able to recover quickly. Similarly the report (Tracking Ghost-Net: Investigating a Cyber Espionage Network, n.d.) demonstrates the findings of an investigation performed to track Ghostnet; a malware for cyberespionage against Tibetan community thought to be of Chinese origin. Over 1,295 infected computers in 103 countries were infected, 30% of which were high value targets (Tracking GhostNet: Investigating a Cyber Espionage Network, n.d.).

In wake of such cases, some countries have taken much advanced steps in order to secure their cyberspace. Efforts such as the development of PceU (Police Central e-Crime Unit) by UK as well as similar stations by Iran and professional training institutes by India (Issues Monitor: Cyber Crime A Growing Challenge for Governments; Volume Eight;12-13, July 2011) are few examples. India developed CERT in 2004 and is now moving on towards other measures such as the activation of JWG (Indo-US Joint Venture Group), which aims to dismantle virtual command centers of terrorist networks (Bhattacharya, 2013). Other countries are also advancing in this regard.

For Pakistan, development of a national CERT would be the first step on the ladder.

Key Issues of Pakistan: The Need for Cert

PKCERT would play a major role in countering terrorist activities within Pakistan. Cyberterrorism constitutes not only attacks targeting critical infrastructure and services but also includes ways of sup-porting suicide attacks and bombings (Bhattacharya, 2013). The serious threat that Pakistan currently faces due to fake gateways and illegitimate SIM cards has just recently been highlighted in electronic and print media (Govt Urged to Enact Laws against Use of Illegal SIMs, 2014). Currently, the government is working on finding and implementing solutions that can eliminate these threats (PTA Hunts Down More Illegal VoIP Gateways, 2013). The pro-cess of tracking down fake SIMs, ensuring their non-existence in future and tracing and inhibiting suspects' communications through web or telecom infrastructure would be made easier with one supreme body dedicated for the purpose.

Pakistan faces yet another threat from cyberterrorism with regards to its neighbouring state India. Independent individuals and private groups from both sides have attempted to deface each other's websites in the past. To name a few, websites of NUML (National University of Modern Languages and Sciences), Quaid-e-Azam Public College Gujranwala, Pakistan Electronic Power Company (PEPCO) and National Bureau Pakistan have been hacked (Aurora, n.d.). While website hacking in itself might not be a very serious threat, such hostile ventures between the two countries where public and military emotions remain aggressive even under normal circumstances can pave way for an even worse situation. The extremes of this can lead to serious cyberterrorism threats. India developed its CSIRT body (CERT-IN) in 2004 as mentioned previously in Section 3. PKCERT, in these circumstances, would strengthen Pakistan's position and help level the two countries' standing in the IT world.

Another domain where PKCERT's services can be considered essential is the nuclear power plants of the country. Cyberattacks on nuclear power plants can cause loss of lives, extreme health damages (due to exposure of radiations), extreme property destruction and economic disaster. These and some other dangers posed by cybercrimes towards nuclear power plants are discussed in (Shea, Gaycken, & Martellini, 2013). PKCERT, once fully functional, can play a role by keeping an eye on cybercrimes related to nu-clear power plants. Generally, these plants are kept devoid of any network access for security and safety purposes. However, threats posed by computer soft-ware vulnerabilities, system malfunction or opera-tor errors (Boulanin & Ogilvie, 2014) still remain under consideration. The incident of STUXNET is common knowledge. Some sources even state that the primary target of this worm was Iran but Pakistan was among those affected (Issues Moni-tor: Cyber Crime A Growing Challenge for Governments; Volume Eight; 12-13, July 2011). It is fortunate enough that Pakistan has not yet witnessed any major cyberattacks but considering its strategic location and political relations, Pakistan must take steps to secure itself in every possible manner. In the developed as well as the developing world, countries are moving towards much advanced steps described under Section 3.

PKCERT would also help Pakistan flourish commercially. This can be a direct result of efficient. IT help services, incident handling and response services, timely notification of malware and vulnerabilities in the wild, forensic labs and the rise of a healthy competitive environment amongst private organizations. In long term services, PKCERT would also help enhance and enforce cybersecurity laws and regulations such as those pertaining to the usage of pi-rated software.

Proposed Framework

The framework that we propose in this section is in-spired from different publications mentioned in Section 2. However, as mentioned in (Killcrece, Kossakowski, Ruefle, & Zajicek, 2003), it is not feasible for any country to pick up guidelines provided in these publications as such and implement them. Cultural and socio-economic conditions are bound to impose some limitations and hence derive the overall process. In this paper, we propose a framework for PKCERT with the above mentioned work as a reference but with significant consideration for Pakistan's socio-economic, cultural and political environment. It is divided into six major steps which range from awareness to professional development. In these six steps, we have considered a team created either from research groups or others working actively for cybersecurity in Pakistan. This team can take an initiative and start a project aiming for the birth of a fully functional and effective CERT in Pakistan. The concerned organization is referred to as PKCERT in this paper. We aim at providing steps for developing a framework at national level which would serve the government, business sector and academic institutions.

Step 1: Awareness Campaign

The first step would be to identify and educate all stakeholders involved in this project. Stakeholders would be all those individuals wanting to participate or to promote cybersecurity in Pakistan. These include IT professionals, students, researchers, professors, media personnel and politicians. A thorough awareness campaign would need to be carried out. Workshops, seminars and training sessions at private and public sector organizations, universities and open-to-all locations such as hotels would be the arranged. The campaign would aim at relaying comprehensive and in depth understanding of the importance of cybersecurity with respect to specific needs. The material for each conference would be different depending on the audience targeted. For IT Professionals, the importance of cybersecurity and CERT with respect to their business needs would be high-lighted.

For other stakeholders, demonstrations regarding how PKCERT could be one of the most efficient enabling tools for the advancement of the country and its citizens' better future would be carried out. For media personnel and

politicians, the key issues de-scribed in Section 3 would be the major curriculum.

This is not a short process spanning over a week or two. Rather, it is a thorough one continuing for at least six months. The end goal would be to enlighten the stakeholders over the importance of CERT in Pakistan and how effectively it would impact each of their needs.

In Pakistan, physical security is a major challenge at present. People in Pakistan are hardly aware of cyberspace and how threats associated with it have an impact on physical security. The awareness campaign will target this issue at grass root level. Securing cyberspace is challenging and not possible with-out reasonable collaboration from the federal and provincial governments. Coordinated and collaborative work from the state and Pakistani citizens is required. A noteworthy concern here is the funding of the awareness campaign. We propose it to come from Educational Institutions and organizations like PISA (Pakistan Information Security Association, n.d.).

Step 2: Funding Strategies

The next major requirement is that of determining suitable funding strategies. Various funding strategies in use by different CERTs around the world are mentioned in (Killcrece et al., 2003). Amongst those options, we propose the last one i.e. combination of membership subscriptions and government sponsor-ship, to suit Pakistan's need at best. On one hand, funding coming purely from government would be infeasible considering the economic conditions in Pakistan. On the other, perceiving funding to come purely from private sector through membership subscriptions would be at most naive, considering that the project has not even kicked off. Also, since PKCERT would be working at national level, complete dependence upon private sector would be impractical.

For a national CERT, a hybrid solution with main authority lying with the government (Ministry of In-formation Technology and Telecommunication) shall be the best possible solution. Policies for membership subscriptions would need to be driven from the Ministry. For this to work however, PKCERT services must be appealing enough and the team be efficient enough to provoke the private organizations to actually step up and subscribe. In an ideal case, PKCERT services would be valuable enough to swivel an environment of competition. That is to say, if telco A is subscribed to PKCERT and availing its services, then its competitors should have no option but to subscribe as well.

In case of the unfortunate scenario described under Step 4, the team must also have contingency funding strategies. To state this clearly, if the government is not ready to fund for the cause, the project should not close at once. Contingency strategies involve looking for external funding sources such as NGOs, research centers and companies working for Information Security.

Step 3: Selection of Services and Cost-Benefit Analysis

The reason we have merged these two into one step is that one dictates the other. Any one of them does not serve as an input or output for the other. Rather, they go side by side. Once the funding strategies have been finalized, an idea of the total budget is in sight.

The services selected would be the ones which give higher benefit compared to the costs involved. In literature, services are divided into three categories (Killcrece et al., 2003), (West-Brown, Stikvoort, Kossakowski, Killcrece, & Ruefle, 2003); Reactive services, Proactive services and Quality Management Services (QMS). Services must be chosen based on best possible quality provision on the targeted constituency (Killcrece, 2004) , (West-Brown et al., 2003), (Haller et al., 2010) Here we suggest that PKCERT focuses on Security Related Information Dissemination (proactive), Risk Analysis (QMS), awareness building and training for the first six months. Since any team cannot be termed as CERT unless it provides some sort of Incident Handling as well (Killcrece et al., 2003), it is suggested that from 7th month onwards, PKCERT starts some incident handling. For this, the latest trends of incidents around the world and within the country should be researched upon first. We have highlighted key national level issues for Pakistan under Section 3. These issues are the ones that must be given high priority. For private organizations, computer security related incidents can then be divided into categories such as DoS attacks, malware outbreak etc. Based upon the latest trends and priorities of member organizations, PKCERT should then select a few incidents for which it would provide handling and response services. In later years, incident handling could be extended for a wider range of services.

While providing these services, it is very essential that a healthy relationship be maintained with the customer companies. Their confidentiality MUST be taken care of through laws and policies and through other possible mechanisms such as classification of information, employee NDAs (confidentiality as a condition for employment) and anonymity of information (Haller et al., 2010). The issue must be addressed with great concern as it is essential for gaining trust and respect and hence for any future progress of PKCERT.

The long term scope of PKCERT will be to serve as a trusted central point of contact, to provide aware-ness and training material to the concerned parties, to give early warnings against vulnerabilities and up-coming threats, incident reporting, mitigation and response and to publish and give security best practices and guidance.

Step 4: Management Approval

The most critical step in Pakistan (and also one of the major constraints) for implementing any national level development activity is getting the approval and authorization from the government. This constrain is such that without having it resolved, any and every other effort would go in vain. For this problem, the solution that we have proposed here lies in steps that precede the activity itself. In other words, we have foreseen spreading awareness as a mechanism to counter this problem.

Once goals of step 1 have been achieved, enough public pressure and media support should ease the process of getting authorization from the Ministry. Additionally, a clear cost-benefit analysis (with benefits weighing heavier on the scale) achieved at step 4 should serve as an efficient means of convincing the authorities.

While this is the best case scenario, the team must also be prepared and MOTIVATED enough for a contingency plan. An example is the legacy of AusCERT as described in (Killcrece et al., 2003) under section 3.3.5. The proposal was rejected by the government in their case but the stakeholders were strongly con-vinced of the need for CERT and hence they decided to build it anyway and started looking for other fund-ing sources.

Step 5: Selection of Constituency

Constituencies refer to the individuals or organizations that would be served by CERT. The publications mentioned in Section 2, all define different possibilities for constituencies. For the case of Pakistan, we suggest government organizations and major private IT organizations (telecom operators, multinational vendors and ISPs etc.) be the target in the beginning. Two of these government organizations have been mentioned in Section 5. Others such as National Engineering and Scientific Com-mission (NESCOM), Khan Research Laboratories (KRL) and security agencies can also be involved. Once PKCERT is fully functional, has gained decent reputation and is financially sound, it may move on towards serving other smaller organizations and even general citizens as well (Sahli, 2007).

Step 6: Staffing and Professional Development

Based on the services decided, professionals must then be trained with due care and diligence. The need and importance of building a team of utmost excellence has already been described in Step 2. Topnotch universities offering IS degrees should be able to pro-vide competitive staff.

The professionals would also need to be trained according to their duties. For example, for the key issues described under Section 3, we propose two specific teams. The team for nuclear plants' safety would comprise individuals having expert knowledge of cybersecurity as well as nuclear physics. Currently in Pakistan, there is no specific academic degree that combines these two fields. How-ever, graduates in nuclear physics, experienced professionals involved in research activity or retired personnel of Pakistan Atomic Energy Commission (PAEC) could be given additional training on cyber-security before hiring. The reverse is also possible i.e. training Information Security graduates and professionals with the required knowledge of nuclear sciences.

Similarly, a team dedicated towards controlling the usage of illegal gateways and unregistered SIMs would comprise individuals having knowledge and experience of cybersecurity and telecom networks. For other services, teams would be trained accordingly. Teams for forensic analysis, malware analysis, malware research and awareness are some examples.

The challenges that would be faced while actually implementing these steps cannot be ignored. As a case study, we have studied particular ones that were faced by South Africa in similar context (Grobler & Bryk, 2010). Some of these can also be foreseen for Pakistan. Political differences, maintaining foreign relations, slow decision making, difficulty in finding investments, need for specialized training as well as huge amounts of equipment are the most noteworthy and hence worrisome.

The first three are major problems and can only be resolved with efficient policies at government level. Recent terrorist attacks have stimulated policy makers into taking meaningful steps. Biometric verification of SIMs is an example. Media can once again play its role in speeding up the process. The remaining three are all finance related. We have de-scribed the funding suitability in section 4.2. As a preliminary action, decent budget from the government would be required. The policy used for different services at various stages would be very important in this regard. If the initial budget is used for the most revenue-generating activities, the subsequent stages could be financially secured.

PKCERT in Perspective: What Would Pakistan Achieve?

Key issues of Pakistan have been highlighted under Section 3. Here we discuss PKCERT's response to these issues with respect to the Incident Response Lifecycle (of Standards & Technology, 2008). Several ways in which safety of nuclear power plants is endangered from cyberspace or computer systems have been described (Shea et al., 2013) and (Boulanin & Ogilvie, 2014). In section 4, we have described the nature of team that can work on these issues. Once established, the team would be dedicated towards research of different cybersecurity and computer security issues related to nuclear plants. It would keep an eye on work being done to ensure cybersecurity of these plants throughout the world by attending international conferences and by coordinating with CERTs of other nuclear states. All useful information such as latest threats, attack pat-terns and mitigation techniques would be delivered to PAEC so that they take appropriate action. The team would also be prepared for any incident in this regard which would be identified and reported to PKCERT by PAEC. The former would have detailed documented procedures, comprising containment, eradication and recovery techniques for each known threat as well as any zero day attacks.

For the case of unregistered SIMs and illegal gate-ways, PKCERT would be collaborating with Pakistan Telecommunication Authority (PTA) and the Police Department. As a trusted entity of the government, this team would collect data of all registered SIMS (CNIC etc.) and legal gateways. It would then, using state of the art technologies, track down all mobile phone activity (not personal information of the citizens but information such as operational mobile phone numbers and gateways within

Pakistan). This way PKCERT's telecom team should be able to promptly identify any SIMs or gateways operating unregistered. PKCERT would then conduct research on material that aids this identification as well as removal. It would particularly be engaged in developing and researching technologies that could come in handy for PTA. The contamination and eradication of this process would be on the shoulders of the Police department.

As for website hacking and other malware commonly found within organizations, PKCERT's role would be very similar to other CERTs around the globe. We discuss here only the case of website hacking. In the planning phase, PKCERT would be involved in spreading awareness about website vulnerabilities and steps for their mitigation. General citizens and organizational representatives would benefit from these open-to-all awareness sessions. Victims could report incidents to PKCERT through channels such as PKCERT's web portal and 24x7 helpline. A team of cybersecurity experts would be ready to respond any time. They would help victims eliminate (containment stage) the danger and recover their web pages. Training on lessons learnt and the importance of backups in such cases would also be the responsibility of this team.

The issues discussed above are the ones most important for Pakistan in the current situation. The overall reduction of website hacking cases in Pakistan and usage of unregistered SIMs and gateways in terrorist attacks would determine the efficiency and achievements of PKCERT. To what extent does PKCERT succeed in achieving its targets can only be determined once some fruitful efforts begin. Some evaluation methods that can be used for assessing performance are given in (Action List for developing CSIRT, 2003).

Conclusion and Future Work

We have proposed a framework for PKCERT. It is envisioned to work at national level, collaborate with government sector and research groups and serve both government and private sectors. Serious and significant efforts are required in order for this to materialize. The current local CERTs in Pakistan are all doing commendable efforts. They are not how-ever, popular enough amongst the technology divisions nor are they working under the direct authority of Ministry of IT. NR3C is working under FIA and could therefore provide an inlet for PKCERT to co-ordinate with agencies.

The scope of this paper is limited and some essential factors have been left out. These can be addressed in future publications. They include identification of critical infrastructure existent within the country, determination and consideration of laws and policies that affect the overall project, complete organizational structure (which would include hierarchy and escalation procedures), integration of security concepts within the basic design of PKCERT (risk management, business continuity planning etc.) and suitable performance evaluation methods. Cybercrimes are not only a threat for the safety of nuclear power plants but can also affect nuclear weapons in several ways (Boulanin & Ogilvie, 2014).

In this paper, we have considered PKCERT's activities only with respect to the category of nuclear plants. To what extent is cyberwarfare capable of affecting nuclear weapons and what role Computer Emergency Response Teams can play in that respect can be explored in future research?

REFERENCES

[1] Action list for developing csirt (Tech. Rep.). (2003). Carnegie-Mellon univ pittsburgh pa software engineering inst.

[2] Aurora, K. (n.d.). Hackers from india and Pakistan in full-blown online war -Retrieved from http://timesofindia.indiatimes.com/ tech/tech-news/Hackers-from-India -Pakistan-in-fullblown-online-war/ articleshow/44766898.cms

[3] Bhattacharya, S. (2013, November). India-Pakistan: Cyber wars analysis." eurasia review, news and analysis. South Asia terrorism portal. Retrieved from http://www.eurasiareview.com/17112014-india-pakistan-cyber-wars-analysis/

[4] Boulanin, V., & Ogilvie, T. (2014, November). Policy brief no 17 - cyber threats and nuclear dangers. Australian National University. Retrieved from https://cnnd.crawford.anu.edu.au/publication/cnnd/4911/policy-brief-no-17-cyber-threats-and-nuclear-dangers

The cert division — sei — cmu. (n.d.). Retrieved from http://www.cert.org/

[5] Cert estonia. (n.d.). Retrieved from https://www.ria.ee/cert-estonia

[6] Cert uk useful documents and links comments. (n.d.). Retrieved from https://www.cert.gov.uk/resources/external-content/useful-links/

[7] Cert uk: what we do. (n.d.). Retrieved from https://www.cert.gov.uk/what-we-do/

[8] Cybercrime law Pakistan. (n.d.). Retrieved from http://zallp.com/cybercrime.html

[9] Cyber security in Estonia. (n.d.). Retrieved from https://www.controlrisks.com/en/newsletters/russia-cis-riskwatch/ issue-6/cyber-security-in-estonia

[10] Govt. urged to enact laws against use of illegal sims.(2014, December). Bureau Report,. Retrieved from http://epaper.dawn.com/DetailImage.php?StoryImage=24 12 2014 182 002

[11] Grobler, M., & Bryk, H. (2010). Common challenges faced during the establishment of a csirt. In Information security for South Africa (issa), 2010 (pp. 1–6).

[12] Haller, J., Merrell, S. A., Butkovic, M. J., & Willke, B. J. (2010). Best practices for national cyber security: Building a national computer security incident management capability (Tech. Rep.). DTIC Document.

[13] Homeland security: About the national cybersecurity & communications integration center. (n.d.). Retrieved from http://www.dhs.gov/about-national-cybersecurity-communications-integration-center

[14] Issues monitor: Cyber crime a growing challenge for governments; volume eight;12-13 (Tech. Rep.). (July 2011). Kpmg International. Retrieved from https://www.kpmg.com/ Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf

[15] Kabay, M. (2005, January). Certs and cirts: Homonyms but not synonyms, part 1.network world. Retrieved from http://www.networkworld.com/article/2328305/lan-wan/certs-and-cirts--homonyms-but-not-synonyms--part-1.html

[16] Khan., M. (2013, July). 7-point action plan proposed for cyber secure Pakistan. Retrieved from http://propakistani.pk/2013/0709/7-point-action-plan-proposed-for -cyber-secure-Pakistan/

[17] Killcrece, G. (2004). Steps for creating national csirts. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University.

[18] Killcrece, G., Kossakowski, K.-P., Ruefle, R., & Zajicek, M. (2003). State of the practice of computer security incident response teams (csirts) (Tech. Rep.). DTIC Document.

[19] Member teams: About apcert / apcert. (n.d.). Retrieved from http://www.apcert.org/ about/structure/members.html Military college of signals. (n.d.). Retrieved from mcs.nust.edu.pk

[20] Najam, S. (2014, Oct). Cybercrimes in pakistan. Retrieved from http://www.dailytimes.com.pk/letters/27-Oct-2014/cyber-crimes-in-pakistan

[21] National response centre for cybercrime. (n.d.). Retrieved from http://www.nr3c.gov.pk/index.html

[22] Nust-csirt. (n.d.). Retrieved from http\%3A\%2F\ %2Fwww.csirt.nust.edu.pk\%2F

[23] Of Standards, N. I., & Technology. (2008). Computer security incident handling guide: Recommendations of the national institute of standards and technology (Tech. Rep.). NIST.

[24] Our services — cert Australia. (n.d.). Retrieved from https://www.cert.gov.au/services

[25] Pakcert :: Pakistan computer emergency response team. (n.d.). Retrieved from http:// www.pakcert.org/defaced/index.html

[26] Pakistan information security association. (n.d.). Retrieved from http://pisa.org.pk/

[27] Pta hunts down more illegal voip gateways. (2013, November). Retrieved from http:// propakistani.pk/2013/11/28/pta-hunts -down-more-illegal-voip-gateways/

[28] Sahli, N. (2007). Tunisia's experience in establishing the first public csirt in Africa, as a case example for developing countries, and some guidelines and schemes for international cooperation..

[29] Shea, T., Gaycken, S., & Martellini, M. (2013). Cyber security for nuclear power plants. In Cyber security (pp. 25–35). Springer.

[30] Tracking ghostnet: Investigating a cyber espionage network. (n.d.). Scribd. Retrieved from http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network

[31] Us-cert: about us. (n.d.). Retrieved from https://www.us-cert.gov/about-us

[32] West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., & Ruefle, R. (2003). Handbook for computer security incident response teams (csirts) (Tech. Rep.). DTIC Document.