CSS CYBER DEFENSE PROJECT

Hotspot Analysis:

Regional rivalry between India-Pakistan: tit-for-tat in cyberspace

Zürich, August 2018

Version 1

Risk and Resilience Team
Center for Security Studies (CSS), ETH Zürich

CSS ETH Zurich

ETH zürich

Author: Marie Baezner

Contact:
Center for Security Studies
Haldeneggsteig 4
ETH Zürich
CH-8092 Zürich
Switzerland
Tel.: +41-44-632 40 25
css@sipo.gess.ethz.ch
www.css.ethz.ch

Analysis prepared by: Center for Security Studies (CSS), ETH Zürich

ETH-CSS project management: Tim Prior, Head of the Risk and Resilience Research Group, Myriam Dunn Cavelty, Deputy Head for Research and Teaching, Andreas Wenger, Director of the CSS

Disclaimer: The opinions presented in this study exclusively reflect the author's views.

Please cite as: Baezner, Marie (2018): Hotspot Analysis: Regional rivalry between India-Pakistan: tit-for-tat in cyberspace, August 2018, Center for Security Studies (CSS), ETH Zürich.

Table of Contents

Executive Summary

Targets:	Indian and Pakistani government websites, government agencies and private firms.
Tools:	Website defacement, spear phishing and malware (Hanove, BADNEWS, MSIL/Crimson, njRAT, DarkComet, Python/Peppy, Android malware).
Effects:	Harassment and annoyance caused by website defacements; financial costs of website defacements; low-level of sophistication, but effective in achieving goals; risk of escalation; targeting non-neighboring states with cyberespionage campaigns.
Timeframe:	1998 - present.

The regional rivalry[1] between India and Pakistan has existed since the two nations achieved independence in the Partition of India. Their relationship is characterized by fierce military and economic competition, resulting in small-scale skirmishes, war, and provocation in the physical and cyber realms. The contested status of the regions of Kashmir and Jammu adds tension to the already strained relationship. To help win small advantages, new technologies are quickly integrated into both nations' strategies; utilizing cyberspace has become a useful tool for both India and Pakistan. Cyberspace has become a space where hacktivists and patriotic hackers[2] from both sides can express their patriotic feelings and denigrate the adversary. Cyberspace also acts as a means for Advanced Persistent Threats (APTs)[3], which are groups that hold highly probable links to state institutions, to spy and gain information on their opponent.

This Hotspot Analysis explores the dynamics of the regional rivalry between India and Pakistan in cyberspace. The report also analyses the effects of these cyber-activities on the domestic, economic, technological and international levels.

Description

The actors involved in India and Pakistan's cyber rivalry thus far are primarily hacktivists and patriotic hackers from both states. Many groups and individuals took part in hacktivism and patriotic hacking to react to physical events and to show their affiliation to their respective state. They targeted both government websites and poorly protected non-governmental websites with website defacement. Both APTs, which are widely believed to be acting in conjunction with the official state, have been involved in cyberespionage campaigns with open source malware delivered through spear phishing emails and/or watering hole attacks.

Effects

This Hotspot Analysis will examine the effects of cyber harassment between India and Pakistan on the countries' already tense relationship. The report finds that at the domestic and social level, the consequences of cyber-activities were largely limited to the inconvenience caused by website defacements. This Analysis also concludes that physical events between the two rivals, such as terrorist attacks or skirmishes on the Line of Control, trigger defacement campaigns from both sides. While website defacement attracts a lot of media attention, its effects are merely an annoyance for most of the population. Website operators were the major economic victims of nationalistic cyber-activities. Website defacement led to economic and reputation losses for website operators that then needed to regain control and reconstruct their websites. Technologically, much of the cyber-activities observed in the India-Pakistan rivalry showed that even with relatively unsophisticated cybertools, both APTs managed to steal information and achieve their strategic goals.

At the international level, the effects of the Indian and Pakistani rivalry in cyberspace were very limited. The primary risk lies in the possibility of escalation. If a state decides it does not want to endure website defacements and/or cyberespionage, it may choose to escalate the rivalry to a physical retaliation. Though the targets of cyberattacks were largely restricted to Indian and Pakistani actors, both APTs also infiltrated networks abroad, most likely to conduct forms of economic espionage.

Policy Consequences

There are a number of general policy recommendations that can be taken from analyzing cyberattacks between India and Pakistan. Any state may improve their cybersecurity by promoting awareness campaigns on spear phishing and website defacement. States may also choose to closely monitor the evolution of the relationship between India and Pakistan, in order to respond effectively in the event of an escalation.

[1] Regional rivalry is understood here as the rivalry between two regional powers and should be differentiated from the rivalry between two Great Powers.

[2] Technical terms are explained in a glossary found in Section 9.

[3] Abbreviations are listed in Section 10.

1 Introduction

India and Pakistan have been regional rivals since their independence in 1947. The unresolved status of the regions of Kashmir and Jammu aggravates the tensions between the two rivals. Their relationship has been punctuated with provocation, conflict, and war. While cyberspace and the internet facilitated communication between India and Pakistan, it also served to increase tensions between the states and their populations. Physical events between India and Pakistan were used as an excuse for hacktivists[4] and patriotic hackers from both sides to launch website defacements campaigns, which often devolved into tit-for-tat defacements. Even though these cyber-activities can increase the tensions between the two regional powers, they have not yet escalated into a conventional conflict. In addition to the hacktivists and patriotic hackers' cyber-activities, Indian and Pakistani actors also conducted cyberespionage against one another, which added pressure to the already tenuous situation.

This Hotspot Analysis explores the rivalry between India and Pakistan in cyberspace. Studying how actions in cyberspace can influence the development of a regional rivalry is particularly relevant today, and can illustrate a number of important lessons for states moving forward. This Hotspot Analysis focuses mainly on website defacements and their dynamic with events in the physical realm, though it does discuss incidents of cyberespionage as well.

In this document, a "hotspot" is understood to be a zone of conflict or tension between states that includes aggravating behavior in cyberspace. A Hotspot Analysis examines specific aspects of cyber-activities to better understand the broader issues in cybersecurity. This Hotspot Analysis is intended to be updated when new developments between India and Pakistan occur and/or new information on cyberespionage campaigns are published. The goal of the updates is to keep the document as current as possible. Hotspot Analyses are also compiled in a broader document that integrates information from other Hotspot Analyses and makes comparisons to provide guidance for cybersecurity policies.

This Hotspot Analysis on the role of cyberspace in the rivalry between India and Pakistan will proceed as follows. In section 2, the Analysis describes the historical background of Indian and Pakistani cyber-activities in relation to historical events linking the two states. The chronology summarizes the major events in the physical realm that triggered cyber-activities.

In section 3, this report details various actors in India and in Pakistan that are involved in cyber-activities: hacktivists and patriotic hackers, and Advanced Persistent Threats (APTs)[5]. The former targets mostly government websites and websites with low levels of security. The latter targets private firms and government agencies. Hacktivists and patriotic hackers in India and Pakistan exploit simple vulnerabilities in websites to deface them. APTs, meanwhile, use more advanced spear phishing and watering hole attacks to infect their targets with freely available, or easily created, malware to spy on their government agencies.

In section 4, the Hotspot Analysis explains the domestic and social effects of cyberattacks on Indian and Pakistani societies. This report shows that website defacement has thus far had a limited impact on both societies, as these cyberattacks are considered to be largely an annoyance. Following that, the Analysis outlines the limited economic effects of these cyberattacks and cyberespionage campaigns. Website defacements only caused minor costs to the website operators, primarily in the form of cybersecurity expenses and reputational costs. Technologically, this Analysis notes that Indian and Pakistani ATPs were able to achieve significant strategic goals using relatively simplistic technological capabilities. Finally, the international effects of the rivalry between India and Pakistan in cyberspace will be discussed. Potential risks primarily consist of the potential risk of an escalation, and cyberespionage campaigns conducted on organizations outside the region, which could damage interstate relations.

In section 5, the Hotspot Analysis suggests some general policy recommendations states may employ to avoid being affected by India and Pakistan's cyber rivalry. It recommends states should improve their own cybersecurity measures and closely monitor the evolution of the conflict in the Indian subcontinent.

[4] Technical terms are explained in a glossary in Section 9.

[5] Abbreviations are listed in Section 10.

2 Background and chronology

The relationship between India and Pakistan is famously tense, and both sides have attempted to win strategic advantage over the years. New technologies, for example, are quickly integrated into standard diplomatic and military doctrine. Pakistan quickly followed India's acquisition of nuclear weapons and increased the stakes of an escalation. Therefore, both saw the opportunity to use cyberspace to harass the adversary with little risk of retaliation. Cyber harassment consists mainly of website defacements and usually occurs on Independence Days and commemoration anniversaries. Cyberattacks are typically low intensity, unsophisticated and cause little damage.

The following chronology provides a partial illustration of the tit-for-tat dynamic that characterizes Indian and Pakistani activities in cyberspace and in relation to specific events in the physical realm.

Rows colored in gray refer to cyber-related incidents.[6]

Date	Event
08.1947	India and Pakistan become independent states, but the status of the northern border provinces of Jammu and Kashmir remain undecided.
10.1947	The Pakistani government supports a Muslim demonstration in Kashmir and starts the 1947-1948 war.
01.1949	India and Pakistan sign the end of the 1947-1948 war and agree on the creation of a Line of Control.
04.1965	Clashes between border patrols on the Line of Control start the 1965 war that ends in January 1966.
1971	East Pakistan achieves independence in the Indo-Pakistani War of 1971. East Pakistan becomes known as Bangladesh.
01.1972	Pakistan starts its nuclear program.
1974	India detonates its first nuclear device.
1988	India and Pakistan agree not to attack their respective nuclear facilities.
1989	Pakistan announces a successful launch of a long-range missile.
1996	India and Pakistan actively try to find a diplomatic solution to ease tensions in the region.
05.1998	India conducts an underground nuclear test in the western state of Rajasthan and Pakistan responds with its first nuclear bomb tests in Baluchistan in the south-west part of Pakistan (BBC News, 2001; Hashim, 2014).
05.1998	Pakistani hackers hack the Indian Bhabha Atomic Research Center's website (Garsein, 2012).
05.1999	Pakistani groups cross the Line of Control in the Kargil region of Kashmir, prompting a retaliatory airstrike from India and starting the Kargil conflict (BBC News, 2001).
10.1999	Pakistani hackers deface an Indian Army propaganda website with messages denouncing torture in Kashmir by the Indian Army (BBC News, 1998).
10.1999	General Musharraf leads a coup to depose Pakistani President Nawaz Sharif.
10.2001	An armed attack on the Kashmiri assembly kills 38 individuals (BBC News, 2001).
23.10.2001	Pakistani patriotic hackers deface two Indian news websites (Majumder, 2001).
13.12.2001	An armed attack on the Indian Parliament kills 14 individuals.
01.2002	Pakistani President Musharraf declares that Pakistan will fight extremism on its territory, but that Kashmir belongs to Pakistan.
2004	The Composite Dialogue Process, a bilateral meeting process, starts between Indian and Pakistani government officials.
07.2008	Indian officials accuse Pakistani Inter Services Intelligence (ISI) of bombing the Indian embassy in Kabul.
26.11.2008	Lashkar-e-Taiba[7], a Pakistani militant group, attacks several targets in Mumbai, including the Taj Mahal Hotel (BBC News, 2018a, 2018b).
27.11.2008	As retaliation for the Mumbai terrorist attacks, Indian hackers deface several Pakistani websites.

[6] A more detailed list of India and Pakistan's rivalry in cyberspace can be found in Annex 1.

[7] Lashkar-e-Taiba is a Pakistani militant group classified as a terrorist group by several countries. Indian authorities accused ISI of actively supporting the group in conducting armed attacks in Kashmir (Bajoria, 2010).

28.11.2008	As retaliation for the defacements, Pakistani hackers deface Indian websites (RFSID, 2016; Ribeiro, 2008).
2009	Pakistani authorities admit that Mumbai terrorist attacks were partly organized from Pakistan, but deny ISI's involvement.
01.2010	Pakistani and Indian troops exchange fire in Kashmir across the Line of Control (Hashim, 2014).
26.11.2010	Indian hackers deface 35 Pakistani websites on the anniversary of the Mumbai terrorist attack.
03.12.2010	Pakistani hackers hack and erase data on the Indian Central Bureau of Investigation website as retaliation for the defacements of November 2010 (Leyden, 2010).
29.11.2011	Indian hackers deface hundreds of Pakistani websites (Kumar, 2011a).
12.2011	A series of tit-for-tat cyberattacks occurs between Indian and Pakistani hackers until February 2012 (Joshi, 2012).
26.01.2012	Independently from the series of cyberattacks mentioned above, Pakistani hackers deface more than 400 Indian websites on Indian Republic Day (Mid Day, 2012).
15.08.2012	Indian hackers deface Pakistani websites on Pakistan Independence Day (Garsein, 2012).
17.03.2013	A Norwegian telecommunications firm reveals that it has been targeted by a cyberespionage campaign possibly coming from India (Fagerland et al., 2013).
26.11.2013	Indian hackers deface several Pakistani websites on the anniversary of the Mumbai terrorist attacks. Pakistan Cyber Army, a Pakistani patriotic hacker group, retaliates by defacing the website of the Indian Central Bank (Kovacs, 2013a).
26.01.2014	Pakistani hackers deface thousands of Indian websites on the Indian Republic Day (Khan, 2014).
26.11.2014	Indian hackers deface several Pakistani government websites on the anniversary of the Mumbai terrorist attacks (Web Desk, 2014a).
26.11.2015	Indian hackers target more than 200 Pakistani websites on the anniversary of the Mumbai terrorist attacks. Pakistani hackers retaliate by defacing the Indian Central Bank website.
06.01.2016	Terrorists attack an Indian Air Force base in Pathankot in northern India.
07.01.2016	Indian hackers retaliate for the terrorist attack in Pathankot with the defacement of Pakistani websites (RFSID, 2016).
03.03.2016	Pakistani authorities arrest an Indian individual suspected of espionage in Pakistan (Shukla, 2017).
15.08.2016	Indian hackers deface more than 50 Pakistani websites on Pakistan Independence Day (TNM Staff, 2016).
18.09.2016	A Pakistani militant group kills 19 individuals in an attack in Uri in Jammu.
23.09.2016	India retaliates for the attack in Uri with surgical strikes.
04.10.2016	Pakistani hackers retaliate for the surgical strikes with the defacement of thousands of Indian websites and Indian hackers claim to have access to Pakistani critical infrastructure networks.
10.04.2017	The Indian individual arrested in 2016 receives the death penalty in Pakistan.
10.04.2017	Indian hackers retaliate with the defacement of hundreds of Pakistani websites to protest against their compatriot's death penalty sentence (Trivedi, 2016).

3 Description

This section describes the multiple actors involved in the rivalry between India and Pakistan in cyberspace, as well as their targets, tools and techniques.

3.1 Attribution and actors

Attribution remains an important challenge in cyberspace. Attribution is usually based on technical evidence coupled with the "*cui bono*" (to whose benefit) logic. A consequence of this is that there will always be small doubts in the attribution process; an actor cannot be identified as the perpetrator of a cyberattack with absolute certainty. Perpetrators can mimic or imitate the tools, techniques and behavior of other actors to confuse the investigators. Moreover, this analysis is based on English language sources from academia, media and cybersecurity firms. These sources reflect a certain point of view that other non-English language sources may not share. Therefore, it is important to bear in mind that attribution in cyberspace is a complex process that may not always be correct.

Actors involved in the Indian and Pakistani tit-for-tat in cyberspace are numerous. In this Hotspot Analysis, they have been divided into two groups: the hacktivists and patriotic hackers, and the Advanced Persistent Threats (APTs). The majority of actors are hacktivists or patriotic hackers, who typically participate in website defacements. These hackers often publicly claim their defacement operations, but it is difficult to tell if they cooperate with similar groups or whether they enjoy state support. It is important to note that some hacktivists and patriotic hackers in India and Pakistan have worked against their own states by defacing their government's websites to denounce corruption or police brutality. Cybersecurity firms have also observed and identified APT groups coming from India and Pakistan, which have conducted more sophisticated cyberattacks than website defacements.

Indian hacktivist and patriotic hacker groups

Indian hacktivists and patriotic hackers[8] were largely identified as acting in defense of Indian interests in cyberspace. Indian hacktivists and patriotic hackers most typically perpetrated website defacement on Pakistani government websites. Some hacktivists and patriotic hackers also claimed ransomware attacks on Pakistani airports and government websites (Shukla, 2017; Trivedi, 2016). These perpetrators were most active on Pakistan Independence Day and the anniversary of the Mumbai terrorist attacks. It remains unclear if the hacktivists and patriotic hackers were groups or individuals and whether they acted in coordination with other hacktivists and patriotic hackers. Some hacktivists and patriotic hackers participated in one defacement campaign and then disappeared. Such behavior suggests that these hacktivists and patriotic hackers were most likely script kiddies. As such, they may have participated in these campaigns for the thrill or to test their knowledge. More patriotic or nationalist hackers tended to reappear from one defacement campaign to another.

The Mallu Cyber Soldiers (MCS) is a hacktivist and patriotic hacker group that stands out due to the number of attacks it has perpetrated. The MCS is a group of Indian cybersecurity experts whose aim is to protect Indian websites from cyberattacks. The MCS was formed in October 2014. The group informed website administrators of vulnerabilities and helped them to restore websites that were defaced. The MCS also retaliated for cyberattacks by defacing Pakistani websites in return. Group members declared that the MCS is totally independent and does not work for the Indian state (International Business Times, 2015).

Pakistani hacktivist and patriotic hacker groups

Pakistani hacktivists and patriotic hackers[9] seem to have been the first ones to use cyberspace to target their opponents in the India-Pakistan rivalry. Similar to Indian hacktivists and patriotic hackers, Pakistani hackers mostly targeted Indian government websites using defacement techniques. Pakistani hacktivists and patriotic hackers were particularly active in retaliation for Indian hacking events, or after specific physical events in Kashmir and Jammu (Trivedi, 2016). As with Indian hacktivists and patriotic hackers, it remains unclear whether Pakistani hacktivists and patriotic hackers were groups or individuals, whether they cooperated among themselves, and their dedication to the cause.

The work of the Pakistan Cyber Army (PCA) was first observed in November 2008 in the defacement of the Indian Oil and Natural Gas Company. The PCA reportedly acted in retaliation for the earlier defacement of Pakistani websites by Indians after terrorists based in Pakistan attacked Mumbai. The PCA used common methods to deface Indian websites. ThreatConnect (2013), a cybersecurity firm, identified at least three members of the PCA. However, it remains unclear whether the group has ties to the Pakistani government or if it acts as an independent entity (RFSID, 2016; ThreatConnect Research Team, 2014).

[8] Indian hacktivists and patriotic hackers are listed in Annex 2.

[9] Pakistani hacktivists and patriotic hackers are listed in Annex 2.

The Indian APT

A Norwegian telecommunications firm discovered an Indian APT[10] in 2013 when the APT targeted the firm with spear phishing emails. Norman Shark and the Shadowserver Foundation, two cybersecurity companies, investigated the Indian APT and found that the group had been active since at least 2010. Various cybersecurity experts have stated that the Indian APT group is not composed of highly sophisticated hackers, as the APT typically used malware available for free. The malware it develops itself was often an amalgamation made by directly copying lines of codes from hacker forums or online public coding projects. Experts also observed that the Indian APT sometimes reused its command and control (C&C) infrastructures and decoy documents in spear phishing emails (Cymmetria, 2016; Fagerland et al., 2013; Settle et al., 2016).

A number of experts have identified this specific APT as an Indian actor because the APT mostly targeted Pakistani organizations, other neighboring countries, and secessionist groups in India. The APT's targets seemed to align with the Indian government's military and political interests. In addition to spying on Pakistan, the APT's activities have refocused China[11] since 2013 or 2014. However, the Indian APT has also targeted firms in Europe (i.e., Telenor in Norway), though these actions might be more akin to economic espionage. Norman Shark and the Shadowserver Foundation's report (2013) also named an Indian cybersecurity contractor that was likely the developer of the malware that targeted Telenor. This finding suggest that the Indian APT outsource some of its work to external contractors. Based on various cybersecurity reports on the Indian APT, it seems very likely that this specific APT has support from the Indian authorities or is part of the Indian state (Cymmetria, 2016; Fagerland et al., 2013; Lunghi et al., 2017; Settle et al., 2016).

The Pakistani APT

Cybersecurity firm Proofpoint exposed the Pakistani APT in its report on Operation Transparent Tribe, which involved a spear phishing campaign against Indian embassies in Saudi Arabia and Kazakhstan in February 2016. Trend Micro revealed to the public that the same Pakistani actor was behind Operation C-Major in March 2016. The Pakistani APT has been active since at least 2012. The APT created counterfeit news websites and sent the link via email to get their victims to click on malicious links to download infected documents. The Pakistani APT used C&C with Pakistani Internet Protocol (IP) addresses. According to cybersecurity experts from Trend Micro, the Pakistani APT used known vulnerabilities to deliver malware and its C&C infrastructure was easy to map. This also indicates relatively unsophisticated cyberattack capabilities. Though the Pakistani APT's targets were also suspiciously in line with the interests of the Pakistani government, neither Proofpoint nor Trend Micro were able to link the Pakistani APT to the Government of Pakistan (Huss, 2016; Kovacs, 2016; Sancho and Hacquebord, 2016).

3.2 Targets

Cyberactors from India and Pakistan targeted roughly equivalent subjects. Hacktivists and patriotic hackers from both states tended to target government institutions and media websites, and their website defacements were largely opportunistic. Hacktivists and patriotic hackers would exploit known vulnerabilities to target unpatched websites (RFSID, 2016). The fact that hacktivists and patriotic hackers mostly attacked government websites reflects the political motives of these actors and indicates they wanted their actions to be noticed.

The Pakistani APT targeted primarily Indian military and diplomatic personnel for the purposes of national security espionage, but also targeted other political and military entities in South Asia (Huss, 2016; Kovacs, 2016). The same was observed for the Indian APT. India's APT conducted mostly cyberespionage against Pakistani private firms and government agencies, but also against international industries. International attacks were likely attempts to gain economic information. The report of Norman Shark and Shadowserver Foundation revealed to the public that the Indian APT's operations did not always align with the interests of the state (Cymmetria, 2016; Fagerland et al., 2013). It is possible that there were a series of poorly-coordinated smaller operations within the Indian government that compromised the APT's efficacy. Similarly, some operations could have been outsourced to a contractor that recycles the same infrastructure for multiple clients. In terms of tracking cyberattacks, all uses of shared infrastructure would appear as if they were perpetrated by the Indian APT.

3.3 Tools and techniques

Actors involved in the tit-for-tat dynamic between India and Pakistan in cyberspace used a variety of cybertools and techniques to achieve their aims. Hacktivists and patriotic hackers used specific tools to find vulnerabilities in websites, and then

[10] The Indian APT is also known as Monsoon, Viceroy Tiger, Dropping Elephant and Patchwork.

[11] It has been reported that Mongolian Intelligence, the Indian Research and Analysis Wing, and the National Technical Research Organisation have a secret agreement on the forensic analysis of raw cyber data that crosses the border between China and Mongolia (Nayar, 2015).

exploited them to deface the site. APTs tended to use spear phishing to get access to their victim's network and then infect them with spying malware.

Website defacement

Cyberattacks directed at the Indian and Pakistani states have most frequently consisted of website defacement by hacktivists and patriotic hackers. Website defacement involves the change of the physical appearance of a website or the redirection of users to another website. This technique is considered to be a form of political activism specific to cyberspace. Perpetrators usually use vulnerabilities in the website structure to access the website server and obtain administration rights. Once the perpetrators have these rights, they can modify the website's appearance. Perpetrators exploit vulnerabilities by various means, often using SQL injection as a means of access. ThreatConnect (RFSID, 2016) reported that some Indian hacktivists used a tool named D3Lt4 to search for SQL injection vulnerabilities.

To deface social media profiles and pages, perpetrators sent phishing emails with counterfeit login pages where the victims would enter their login credentials. The perpetrators would then use the stolen information to access their victim's social media accounts.

Spear phishing

Spear phishing consists of sending an email that appears to come from a trusted contact or organization. Targets would be tricked into downloading attachments infected with malware or into clicking on a link to download a malicious file or to a fake website. These counterfeit websites could be fake login pages or a website encouraging users to download specific infected files.

Hacktivists and patriotic hackers in India and Pakistan used spear phishing to get access to social media accounts (RFSID, 2016). The Indian and Pakistani APTs used spear phishing to trick victims into clicking on malicious links or downloading infected attachments that would download malware in the users' computers (Fagerland et al., 2013; Huss, 2016).

Malware

The Indian and Pakistani APTs used multiple types of malware in their campaigns. The following list is only a sample of the malware utilized by the two APTs, but it nevertheless gives an accurate impression of the types of malware that both APTs employ.[12]

Indian APT's malware

Hanove malware

The Hanove[13] malware was found in 2013 in a cyberespionage campaign targeting industries in Norway, Pakistan, USA, Iran, China, Taiwan, Thailand, Jordan, Indonesia, United Kingdom, Germany, Austria, Poland and Romania. The Hanove malware is a second-stage malware that is often dropped by a first-stage Trojan named Smackdown. The Hanove malware is designed to steal documents, to register keystrokes, and to take screenshots. The malware then uploads the stolen information and data to a remote server (Fagerland et al., 2013; Symantec Security Response, 2013; ThreatConnect Research Team, 2013).

BADNEWS malware

BADNEWS is a first stage malware that is usually delivered by spear phishing emails and packaged in a malicious attachment. The BADNEWS malware is a backdoor that can take screenshots, record keystrokes, and self-update. It can be used to monitor USB-drives, as well as download and execute files. The BADNEWS malware uses RSS feeds, forums and blogs as C&C infrastructures. Since its first observation in 2016, the BADNEWS malware has been updated to obfuscate C&C information (Levene et al., 2018; Lunghi et al., 2017; Settle et al., 2016).

Android spying application

The cybersecurity firm CrowdStrike (2016) observed in 2015 that the Indian APT also employed spying applications on Android phones. The Indian APT developed an application called Zonero, which is a customized variant of AndroRAT. The latter is a Remote Administration Tool (RAT) available for free on the internet.

Pakistani APT's malware

MSIL/Crimson malware

The Pakistani APT developed counterfeit blogs and news websites with links to articles that would download MSIL/Crimson. This malware is a first-stage malware used to download other RATs. MSIL/Crimson can record keystrokes, steal login credentials saved in internet browsers, activate webcams, take screenshots, and steal emails from Microsoft Outlook (Huss, 2016; Sancho and Hacquebord, 2016).

[12] A more extensive list can be found in Annex 3.

[13] Hanove is also known as HangOver, HangOve and Trojan.Hangover.

Android spying applications

Experts from Trend Micro (2018) reported that a Pakistani threat actor used malicious Android applications (i.e., PoriewSpy, freeCall, BatterySavor) in their operations. The experts concluded that some of these applications were developed from DroidJack and SandroRAT, which have been available for free on hacker forums since 2013. These malicious applications can steal text messages, call logs, contacts, location, SD card information, and file lists, as well as record voice calls. The applications were directly downloaded from malicious websites created by Pakistani actors and were targeted towards Android users in India (Xu and Guo, 2018).

In 2018, the mobile security firm Lookout (2018) issued a report on a malicious application on Android and another iOS. Lookout called the Android application Stealth Mango and the iOS application Tangelo. The Pakistani APT, using fake Facebook personas, would start a conversation with their targets on Facebook Messenger and push them to download a video call application infected with Stealth Mango or Tangelo. The malicious application enabled the perpetrators to steal more than 30 GB of data (government communications, pictures of official documents, GPS coordinates, etc.). Lookout concluded this espionage campaign was likely run by the Pakistani military (Blaich and Flossman, 2018; Lookout, 2018; O'Neill, 2018).

The Indian Army issued a warning in February 2016 regarding a chat application popular amongst Indian Army personnel: SmeshApp. The Indian Army accused ISI of developing the application to gain access to military personnel's smartphones. The application could collect GPS locations, photos, emails, messages and call histories (Cimpanu, 2016a).

4 Effects

This section analyzes the effects of the cyberattacks between India and Pakistan on both Indian and Pakistani societies, the economic costs of this cyber-conflict, and technological implications.

Additionally, the consequences of cyberattacks on the international level will be examined. Increasing levels of interference from non-state actors risks escalating regional tensions into a conventional conflict, and portends cyberespionage campaigns that span far beyond the Indian and Pakistani borders.

4.1 Social effects

The most typical type of cyberattack used to denigrate the opposing state was website defacement. Website defacements are more of a disruption or annoyance, and they do not tend to result in lasting or physical damage. Nevertheless, the inconvenience created by website defacement affected the users of the defaced websites, especially because hacktivists and patriotic hackers often targeted government agencies' websites. Given the public nature of the attack, website defacements typically garnered more attention than other types of cyberattacks, such as cyberespionage. The increased visibility may also imply that defacements are a more significant attack on a country than the act itself should objectively merit. Perpetrators of website defacements usually took responsibility for their acts and relied on media coverage to further spread their message. Furthermore, the intense media scrutiny resulting from website defacements can be manipulated to generate fear among the targeted population. These attacks acted as reminders for the rival population that they are at risk and cannot protect themselves from cyberattacks.

Often, the website defacements were a reaction to specific events, like a cricket game or the arrest of an Indian individual in Pakistan. Real-world incidents would trigger a response from the hacktivists and patriotic hackers to either express their dissatisfaction with events, denounce a situation that they consider to be unfair, or simply express their patriotism. For example, Indian hacktivists and patriotic hackers regularly targeted Pakistani websites with Indian patriotic messages (Balduzzi et al., 2018; Bussoletti, 2018; RFSID, 2016; Web Desk, 2014b).

4.2 Economic effects

The economic effects of the tit-for-tat dynamic between India and Pakistan in cyberspace are limited. Consequences primarily consisted of the costs of

website defacement for the owners of affected websites. These losses are not materially different from the price of similar Distributed Denial of Service (DDoS) attacks. For private businesses, defacements result in lost customers due to the unavailability of the webpages and damages to the businesses' reputation. For other targets, such as government agencies, websites defacement generates a loss of trust from the websites' users. The fact that website owners failed to proactively address vulnerabilities in their website suggested to the users that the website and its owners were not trustworthy (Paladion Networks, 2015).

4.3 Technological effects

Cybersecurity experts that studied APT groups from India and Pakistan found that it was easy to conduct significant cyberespionage campaigns using relatively unsophisticated and readily available cybertools. The experts exposed that Indian and Pakistani APTs either built their malware from codes copied directly from hacker forums or open source projects, or used malware that was freely available on the internet. The widespread availability of malicious cybertools and codes is not new, but to witness actors - some with alleged state sponsorship - capitalize on these instruments is rather unique. Combining relatively simple malware with spear phishing and watering hole attacks, Indian and Pakistani APT groups managed to steal a significant volume of information from their victims. These cases demonstrated that APT groups did not have to rely on highly complex technology to achieve their goals. An important caveat to this lesson is that experts also concluded populations in India and Pakistan were not well-versed in cybersecurity issues. In part, this is due to a simple lack of awareness; APT groups appeared to recognize unsophisticated cybertools were enough to achieve their goals (Cymmetria, 2016; Huss, 2016; Sancho and Hacquebord, 2016; Settle et al., 2016).

4.4 International effects

The international consequences of India and Pakistan's rivalry in cyberspace are minimal. The main risk presented by continued cyberattacks is a possible escalation of real-world events through the actions of non-state actors on the internet. Additionally, cyberespionage campaigns directed towards third party states hold the potential to significantly damage relations between India, Pakistan, and the rest of the world.

Non-state actors

While website defacements thus far have largely been considered a mere annoyance, there is a risk that defacement may escalate existing tensions and prompt a conventional conflict. Website defacements were typically conducted by non-state actors, and it remains difficult to evaluate the relationship between these shadowy hackers and the official state apparatus. Even if non-state actors are completely independent from their parent state, their motives were often patriotic and responded to events in the physical world that the hackers considered an affront to their nation. In the case of India and Pakistan, these cyberattacks are largely carried out by the population, not the official state and risk to solidify the conflict at the population level. While these small-scale attacks are clearly derived from the bottom-up, the target state may perceive the attacks as being conducted by the official government. This is of particular risk as cyberattacks evolve and seek to target more advanced targets (e.g., critical infrastructures), or if continuous website defacements become too disruptive to society (Lin, 2012). India and Pakistan have nuclear capabilities and an escalation from cyberspace to conventional conflict also brings the risk of a further escalation into a nuclear conflict.

That being said, the effects of cyberattacks have been constrained to the cybersphere for the last 15 years. Hacktivists and patriotic hackers defaced websites as a response to physical events like a terrorist attack or skirmishes along the Line of Control, but thus far, no website defacement has prompted a real-world response. Nevertheless, cyberattacks of low intensity, like website defacements, will most likely continue between Indian and Pakistani hacktivists and patriotic hackers. This pattern will continue to increase the risk of misinterpretation and escalation.

International cyberespionage

The Indian APT conducted several cyberespionage campaigns, primarily targeting Indian secessionist groups and Pakistani actors. However, this APT also targeted firms and government institutions outside India and Pakistan. The targets appeared to be government and industry-related institutions in neighboring countries, the Middle East, and the West. (Crowdstrike, 2016; Lunghi et al., 2017; Symantec Security Response, 2013). Espionage and cyberespionage may be at least tolerated on the international level for national security purposes, but no such allowance exists for economic espionage. Economic cyberespionage campaigns risk straining relationships between the targeted states and India. Furthermore, targeted private firms may seek governmental support, which would open the Indian APT up to retaliation. This is also true of regular espionage, if a neighboring or partner country of India discovered that it was the target of that APT.

5 Policy Consequences

This section suggests general measures states can implement to reduce the risks of being impacted by similar malicious cyber-activities, and avoid the examples of India and Pakistan.

5.1 Improving cybersecurity

Many cyberattacks between Indian and Pakistani actors started with spear phishing campaigns. Spear phishing emails served to lure the victim to download an attachment infected with malware or to click on a link to direct the victim to a malicious website. It is, therefore, necessary to raise awareness among users about such dangers. Sensitization campaigns could help users more easily recognize spear phishing emails and watering hole attacks. Institutions could also implement standardized procedures in case an employee opens a malicious attachment or clicks on a malicious link. A predetermined response would help institutions to deal faster with the intrusion.

Implementing an email authentication system, like the Sender Policy Framework (SPF), could provide a technological solution to problems of phishing. The SPF certifies the authenticity of the sender of an email, making it easier to identify spear phishing emails.

In the case of website defacement, there is no specific measure that could guarantee that a website will not be defaced. However, there are tactics that website owners can implement to reduce their risk. Website owners could conduct regular penetration tests to detect vulnerabilities. In addition, website defacement monitoring and detection tools could help website owners react faster in the event of a defacement.

5.2 Monitoring relations between India and Pakistan

The tensions between India and Pakistan have been omnipresent since the two nations gained independence in 1947. Since then, wars and skirmishes have marred the evolution of their relationship. Cybertools only brought new ways to harass and spy on the other state. However, the advent of cyber harassment brought new actors into the fold, which increases the risk of a misinterpretation in cyberspace. If understood as an act perpetrated by the opposing state, and not members of the public, cyber harassment campaigns could escalate existing tensions into conventional conflict. As such, outside states should closely monitor India and Pakistan's relationship, as well as the actions of non-state actors in cyberspace, to be able to respond in a timely and effective manner in the case of an escalation.

6 Annex 1

Non-exhaustive list of cyber-incidents related to India and Pakistan disputes.

G = Government and government institutions, M = Media, MIL = Military institutions, O = Others, PP = Political Party				
Date	**Victim(s)**	**Type of victim(s)**	**Alleged perpetrator**	**Technique/Tool**
05.1998	India Bhabha Atomic Research Center's website	G	Unknown Pakistani hackers	Defacement (Garsein, 2012)
10.1999	Website of the Indian Army unit stationed in Kashmir	MIL	Unknown Pakistani hackers	Defacement (BBC News, 1998)
10.2001	2 US government websites	G	Gforce Pakistan and Pakistani Hackerz Club	Defacement (Majumder, 2001)
23.10.2001	2 Indian news websites	M	Gforce Pakistan and Pakistani Hackerz Club	Hack (Majumder, 2001; Maness and Valeriano, 2017)
12.07.2003	Some Pakistani websites	Unknown	Unknown	Defacement (Maness and Valeriano, 2017)
11.2008	Pakistani pages on the social media Orkut	O	HMG (Indian haccker)	Hack (Livemint, 2008)
27.11.2008	Pakistan Oil and Gas Regulatory Authority	G	Indian hackers named HMG	Defacement (Livemint, 2008; Maness and Valeriano, 2017)
27.11.2008	Pakistani websites	Unknown	Unknown Indian hackers	Defacement (Maness and Valeriano, 2017; Ribeiro, 2008)
28.11.2008	Indian Oil and Natural Gas Corporation, Indian Railways, Indian Institute of Remote Sensing, and school websites	G	PCA	Defacement (RFSID, 2016; Ribeiro, 2008)
24-25.12.2008	Indian transportation website	G	Unknown	DDoS (Maness and Valeriano, 2017)
01.2009	Indian popular music download website	O	Unknown Pakistani hackers	Infected with malware (Geers et al., 2014)
02.2009	600 computers in the Indian Ministry of External Affairs	G	Unknown	Hack (Center for Strategic and International Studies, 2018)
08.2010	Indian industry Vijay Mallya	O	Pakistani hackers claiming to be PCA	Hack (ThreatConnect Research Team, 2014)
2-12.09.2010	Indian websites	Unknown	Unknown Pakistani hackers	Defacement (Maness and Valeriano, 2017)
2-12.09.2010	Pakistani websites	Unknown	Unknown Indian hackers	Defacement (Maness and Valeriano, 2017)
26.11.2010	35 Pakistani websites, including the Pakistani Navy, the National Accountability Bureau, the Ministry of Foreign Affairs, the Ministry of Education, the Ministry of Finance websites	G, O	Indian Cyber Army	Hack (Leyden, 2010)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool
03.12.2010	Indian Central Bureau of Investigation and National Informatics Centre websites	G	PCA	Defacement and data erased (RFSID, 2016)
05.2011	PCA website	O	Indian Cyber Army	Hack (ThreatConnect Research Team, 2014)
14.10.2011	Pakistani embassy in China website	G	Vicky Singh	Defacement (Kumar, 2011b)
15.10.2011	Indian Cyber Crime Investigation Cell in Mumbai website	G	Shadow008	Defacement (Passeri, 2011a)
29.11.2011	More than 100 Pakistani websites, including the Peshawar Electric Supply Company, the Ministry of Information and Broadcasting, the Government of Pakistan and the Pakistan Navy websites	G	Godzilla	Defacement (Kumar, 2011a)
08.12.2011	Dawn.com (Pakistani news website)	M	Indishell	Hack and release of stolen information (Kumar, 2011c)
09.12.2011	Indian National Congress website	G	KhantastiC (part of PCA)	Defacement (Passeri, 2011b)
20.12.2011	More than 800 Pakistani websites	Unknown	Indishell	Defacement (Passeri, 2011c)
04.01.2012	30 Pakistani websites	Unknown	Indishell	Defacement (Kumar, 2012)
26.01.2012	More than 400 Indian websites	Unknown	ZCompany Hacking Crew	Defacement (Mid Day, 2012)
03.2012	More than 100 Indian websites	G, Unknown	Unknown Pakistani hackers	Defacement (Geers et al., 2014; Joshi, 2012)
07.2012	More than 10,000 emails of Indian government officials	G	Unknown	Hack (Center for Strategic and International Studies, 2018)
15.08.2012	Pakistani websites	Unknown	Unknown Indian hackers	Defacement (Garsein, 2012)
23.09.2012	Karachi stock exchange and Pakistani Army websites	G, O	Godzilla	Hack (Passeri, 2012)
15.02.2013	Indian websites	Unknown	ZCompany Hacking Crew and the Anonymous	Defacement (Kovacs, 2013b)
05.03.2013	Unofficial ISI website	G	Godzilla	Hack (Wei, 2013)
11.03.2013	Pakistani websites	Unknown	Godzilla	DDoS and dump passwords for the websites (Kovacs, 2013c)
17.03.2013	Telenor, a Norwegian telecommunication company	O	The Indian APT	Use of custom malware for cyberespionage (Fagerland et al., 2013)
06.07.2013	Several websites of the Government of Goa	G	H4x0r HuSsY	Hack (Sharma, 2013)
14.07.2013	Pakistani Ministry of Education website	G	Indi-Heax	Defacement (E Hacking News, 2013a)
07.08.2013	Indian database of Bharat-Sanchar Nigram Ltd, owned by the Indian State	G,O	ISI	Cyberespionage (joji, 2013)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool
13.08.2013	Indian Railways website	G	PCA	Defacement (RFSID, 2016)
29.09.2013	20'000 Indian websites	Unknown	Dr@cul@ and Muhammar Balil	Defacement (Waqas, 2013a)
02.11.2013	Maharashtra Police Academy website	G	Gujjar (part of PCA)	Defacement (Waqas, 2013b)
26.11.2013	Pakistani websites, including the Lodhran District Police website	G and unknown	Unknown Indian hackers	Defacement with messages in honor of the victims of the Mumbai terrorist attacks (Kovacs, 2013a)
26.11.2013	Indian Central Bank and Commissioner of Customs in Lucknow websites	G	PCA	Defacement (Kovacs, 2013a)
09.12.2013	More than 30 websites of the government of Rajasthan	G	H4x0r HuSsY	Defacement (E Hacking News, 2013b)
26.01.2014	More than 2,000 Indian websites	Unknown	Pakistani hackers	Defacement (Khan, 2014)
27.01.2014	Indian Railways website	G	H4$4!n H4xor	Defacement (E Hacking News, 2014a)
29.01.2014	100 Pakistani websites	Unknown	Unknown Indian hackers	Defacement (Khan, 2014)
4-5.02.2014	Indian websites	Unknown	Unknown Pakistani hackers	Defacement (Kovacs, 2014)
19.02.2014	India.gov.in	G	ZCompany Hacking Crew	Defacement with messages in favor of Kashmir (Passeri, 2014a)
05.03.2014	Swami Viveksand University website	O	PCA	Defacement (RFSID, 2016)
06.03.2014	Uttar Pradesh University website	O	PCA	Defacement (RFSID, 2016)
20.03.2014	Indian Central Bank website	G	PCA	Defacement (RFSID, 2016)
19-20.04.2014	Bijar BJP and BJP leader websites	PP	Muhammar Balil	Defacement (E Hacking News, 2014b)
19.04.2014	Bangalore City Police website	G	H4x0r10ux m1nd	Defacement (Waqas, 2014a)
11.05.2014	Indian Railways website	G	rOOx	Defacement (Passeri, 2014b)
27.05.2014	Taj Mahal official website	O	H4$4!n H4xor Hunter Khan	Defacement (E Hacking News, 2014c)
08.10.2014	Pakistan People's Party website	PP	Black Dragon	Defacement with an Indian flag (Web Desk, 2014b)
09.10.2014	Indian government websites	G	Unknown Pakistani hackers	Defacement (Kumar Jha, 2014)
09.10.2014	Pakistani Railways, Pakistani universities and Pakistani Electric Power Company websites	G, O	Unknown Indian hackers	Defacement (Kumar Jha, 2014)
19.10.2014	Ludhiana rural police	G	Virkid	Defacement (Waqas, 2014b)
28.10.2014	BJP in Rajkot website	PP	ZCompany Hacking Crew	Defacement (Passeri, 2014c)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool
06.11.2014	22 Indian websites	Unknown	Team MadLeets	Defacement with messaging on the violation of civil rights in Kashmir (Web Desk, 2014c)
26.11.2014	Pakistani Meteorological Department and the Lahore High Court websites	G	Unknown Indian hackers	Defacement (Web Desk, 2014a)
02.07.2015	Indian National Institute of Technology in Raipur	G	Pakistani hacker named Faisal Afzal (part of PCA)	Defacement (Dawn.com, 2015)
15.08.2015	Thermala Eco Tourism website (India)	O	Unknown	Hack (RFSID, 2016)
15.08.2015	120 Pakistani websites	Unknown	Indian Cyber Pirates, Indian BlackHats and Mallu Cyber Soldiers	Hack (RFSID, 2016)
28.09.2015	Kerala state government website (India)	G	PCA or Faisal Afzal	Hack (RFSID, 2016)
29.09.2015	More than 100 Pakistani websites	Unknown	Mallu Cyber Soldiers	Hack (RFSID, 2016; Shukla, 2017)
03.10.2015	Pakistani government websites	G	Hell Shield Hackers (India)	Defacement (DNA Web Team, 2015)
20.10.2015	Kalkota Passport Office	G	Pak Cyber Experts	Defacement (FIA, 2015)
31.10.2015	Several Indian colleges websites	O	VirusHacker (Pakistan)	Defacement (Mehta, 2015)
03.11.2015	Indian Army personnel	MIL	Unknown	Smartphone Hacks (RFSID, 2016)
26.11.2015	More than 200 Pakistani websites	Unknown	Kerala Cyber Warriors, Mallu Cyber Soldiers and Team India Black Hats	Hack (RFSID, 2016; Shekhar, 2015)
26.11.2015	Indian Central Bank website	G	Unknown Pakistani hackers	Hack (Cimpanu, 2015)
27.11.2015	Pakistani government websites	G	Unknown Indian hackers	Defacement (Vijay, 2015)
27.11.2015	Jabalput police website (India)	G	PCA	Defacement using the Pakistani flag and slogans (Passeri, 2015)
07.01.2016	Pakistani websites	Unknown	Unknown Indian hackers	Hack (RFSID, 2016)
02.2016	Smartphone applications named SmeshApp, WeChat and Line that are popular among Indian Army personnel	MIL	Unknown	Malicious applications (Cimpanu, 2016a)
06.02.2016	Indian Revenue Service	G	PCA	Defacement (Press Trust of India, 2016)
11.02.2016	Indian embassies in Saudi Arabia and in Kazakhstan	G	Pakistani actors identified in the Trensparent Tribe report	Spear phishing (Huss, 2016)

Date	Victim(s)	Type of victim(s)	Alleged perpetrator	Technique/Tool
18.03.2016	Indian government officials	G	Pakistani actors identified in the Trensparent Tribe report	Spear phishing and watering hole attacks (Kovacs, 2016)
11.06.2016	8 Indian embassies websites	G	Pakistani hackers named Intruder and Romantic	Defacement (Cimpanu, 2016b)
02.08.2016	E-banking system of an Indian bank	O	Faisal Afzal	Hack (Shekhar, 2016a)
15.08.2016	More than 50 Pakistani websites	Unknown	Kerala Cyber Warriors	Defacement (TNM Staff, 2016)
04.10.2016	More than 7,000 Indian websites	Unknown	Pakistan Haxors Crew	Hack (Purani, 2016; Trivedi, 2016)
04.10.2016	Pakistani government network	G	Telangana Cyber Warriors (India)	Ransomware (Shekhar, 2016b; Trivedi, 2016)
04.10.2016	Pakistani critical infrastructure networks	G, O	Officials from the Indian National Cyber Safety and Security Standards	Hack and implants (FP Staff, 2016)
01.01.2017	Indian Special Forces, the National Security Guard, website	MIL	Pakistani hacker named Alone Injector	Defacement (Monitoring Desk, 2017)
02.01.2017	Three Pakistani airport websites	G, O	Unknown Indian hackers	Ransomware (Monitoring Desk, 2017; Shukla, 2017)
02.2017	Indian Central Bureau of Investigation and Indian Army officers	G, MIL	Unknown Pakistani hackers	Spear phishing (Center for Strategic and International Studies, 2018)
04.2017	Pakistani government websites	G	Unknown Indian hackers	Unknown (Shukla, 2017)
24.04.2017	Pakistani Railway Ministry website	G	Indian hacker named Code Man	Hack (D'Mello, 2017)
25.04.2017	10 Indian University websites	G, O	Pakistan Haxors Crew	Hack and defacement (D'Mello, 2017)
03.08.2017	Official Pakistani government website	G	Indian hacker named Ne0-H4ck3r	Defacement with Indian anthem (Shukla, 2017)
12.2017	Indian Android users	Unknown	Unknown	Malicious applications (Xu and Guo, 2018)
01.2018	Indian Unique Identification Authority	G	Unknown	Theft of personal data of more than one billion individuals (Center for Strategic and International Studies, 2018)
02.2018	Kerala state government website	G	Pakistani hacker named Fajal1337	Hack (Bussoletti, 2018)
02.2018	More than 250 Pakistani websites, including the Pakistani Railway Ministry website and the Pakistani Presidential website	G, Unknown	Mallu Cyber Soldiers	Hack (Bussoletti, 2018)

7 Annex 2

Non-exhaustive list of hacktivists and patriotic hackers by country:

India	Pakistan
Black Dragon	Alone Injector
Code Man	Dr@cul@
Godzilla also known as G.O.D	Faisal Afzal
Hell Shield Hackers	Gujjar (part of Pak Cyber Pyrates)
HMG	H4$n4!n H4xor Hunter Khan
India Cyber Pirates	H4x0r HuSsY
Indian BlackHats	H4x0r10ux m1nd
Indian Hackers Godziila Volcanium	Intruder
Indian Hackers Online Squad	MaDLeets
Indishell	Muhammad Balil (part of Pak Cyber experts)
Kerala Cyber Warriors	Pak Cyber Eaglez
Lulzsec India	Pak Cyber Experts also known as Team Pak Cyber Experts
Mallu Cyber Soldiers	Pak Cyber Pyrates
Mr Z	Pakistan Haxors Crew
Ne0-H4ck3r	Pakistani Cyber Attackers
Nomcat	Pakistan Cyber Army
Team Indi-Heax	Romantic
Telangana Cyber Warriors	rOOx (part of MaDLeeTs)
Vicky Singh	Shadow008
	Virkid (part of MaDLeeTs)
	Virushacker
	Z Company Hacking Crew
	Zindabad (part of PCA)

8 Annex 3

Non-exhaustive list of malware used by both Indian and Pakistani APTs:

Indian APT's malware

Malware	Features
Smackdown	Gathers information on the operating system (Fagerland et al., 2013).
Hanove	Steals documents, keylogger, takes screenshots (Fagerland et al., 2013).
Meterpreter	Metasploit payload (Cymmetria, 2016).
Zonero	Malicious Android application (Crowdstrike, 2016).
BADNEWS	Backdoor that takes screenshots, keylogger, self-updates, monitors USB-drives, downloads and executes files (Lunghi et al., 2017; Settle et al., 2016).
Unknown Logger public V1.5	Public and free backdoor that steals login credentials saved on browsers, keylogger, takes screenshots, spreads itself, downloads a second stage malware (Settle et al., 2016).
AutoIt Backdoor	Also known as File Stealer. It gathers information on the operating system, updates itself, escalates privileges, exfiltrates files and steals passwords from the Chrome browser (Lunghi et al., 2017; Settle et al., 2016).
TinyTyphoon	Backdoor based on the MYDOOM worm code. TinyTyphoon can find and upload documents and download a second stage malware (Settle et al., 2016).
A variant of the xRAT Trojan	Open-source RAT (Lunghi et al., 2017).
NDiskMonitor	A customized backdoor that lists files and drives, and downloads and executes files (Lunghi et al., 2017).
Socksbot	Backdoor that takes screenshots, writes and executes programs (Lunghi et al., 2017).

Pakistani APT's malware

Malware	Features
Bitterbug	Backdoor first observed in 2013, which can upload and download files (Barger et al., 2014).
MSIL/Crimson	First stage malware that is a keylogger, steals login credentials, and activates webcams, takes screenshots and steals emails (Huss, 2016; Sancho and Hacquebord, 2016).
njRAT	RAT also known as Bladabindi or Zapchast. njRAT collects documents, makes screenshots, gathers login credentials, records keystrokes, deletes files and activates the webcam and microphone. njRAT can avoid antivirus detection because of its encrypted architecture (New Jersey Cybersecurity & Communications Integration Cell, 2017). The use of njRAT has also been observed in the Syrian civil war.[14]
DarkComet RAT	RAT developed by a French hacker in 2011, made freely available on surveillance forums. The RAT activates webcams, disables the detection notification of antiviruses, records keystrokes, steals login credentials, deletes and controls files, and starts DDoS attacks (New Jersey Cybersecurity & Communications Integration Cell, 2016). The DarkComet RAT has also been observed in the Syrian civil war.[15]
Luminosity Link RAT	RAT that was available for free online. Luminosity Link opens files, records keystrokes and activates webcams (HelpNetSecurity, 2018; Huss, 2016).
Python/Peppy	Python/Peppy registers keystrokes, exfiltrates files, updates itself, takes screenshots, downloads remote files and executes them (Huss, 2016).
Bezigate	Backdoor that steals operating system information and files (Huss, 2016; Windows Defender, 2011).
Meterpreter	Metasploit payload (Cymmetria, 2016; Huss, 2016)
Beendoor	Trojan that takes screenshots (Huss, 2016).

[14] For more information on the cybertools used in the Syrian civil war see: Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, October 2017, Center for Security Studies (CSS), ETH Zürich.

[15] Ibid.

DroidJack and SandroRAT-based malicious applications	A range of applications that access and execute calls, SMS, contacts, camera, microphones and enables and disables the Wifi receiver (Xu and Guo, 2018). The use of these malicious applications was also observed in the Syrian civil war.[16].
PoriewSpy	Malicious application which steals SMS, call logs, contacts, GPS location, SD Card file lists and records voice calls. The malware was developed in an open-source project in 2014 (Xu and Guo, 2018)
Breach RAT	RAT that takes screenshots and records key strokes (Cimpanu, 2016c).
Stealth Mango	Malicious application for the Android operating system which steals pictures, videos and audio files stored on the phone, calendar events, contact lists from other applications, call logs, SMS logs, and GPS coordinates. The malicious application is downloaded through Facebook Messenger (Lookout, 2018).
Tangelo	Malicious application for the Apple operating system which steals SMS messages, call logs, browser histories, pictures, videos, and GPS coordinates. The malicious application is downloaded through Facebook Messenger (Lookout, 2018).

[16] For more information on the cybertools used in the Syrian civil war see: Baezner, Marie; Robin, Patrice (2017): Hotspot Analysis: The use of cybertools in an internationalized civil war context: Cyber activities in the Syrian conflict, October 2017, Center for Security Studies (CSS), ETH Zürich.

9 Glossary

Advanced Persistent Threat (APT): A threat that targets critical objectives to gain access to a computer system. Once inside a network, it tries to remain hidden and is usually difficult to remove when discovered (Command Five Pty Ltd, 2011; DellSecureWorks, 2014).

Backdoor: An element of software code that allows hackers to remotely access a computer without the user's knowledge (Ghernaouti-Hélie, 2013, p. 426).

Command and Control infrastructure (C&C): A server through which the person controlling malware communicates with it in order to send commands and retrieve data (QinetiQ Ltd, 2014, p. 2).

Distributed Denial of Service (DDoS): The act of overwhelming a system with a large number of packets through the simultaneous use of infected computers (Ghernaouti-Hélie, 2013, p. 431).

Hack: Act of entering a system without authorization (Ghernaouti-Hélie, 2013, p. 433).

Hacktivism: Use of hacking techniques for political or social activism (Ghernaouti-Hélie, 2013, p. 433).

Internet Protocol (IP) address: A numerical address assigned to each device that uses the internet communications protocol, allowing computers to communicate with one another (Internet Corporation For Assigned Names and Numbers, 2016).

Keylogger: Feature that traces keystrokes without the knowledge of the user (Novetta, 2016, p. 56).

Malware: Malicious software that can take the form of a virus, a worm or a Trojan horse (Collins and McCombie, 2012, p. 81).

Metasploit Framework: An open source penetration testing tool to uncover exploits by simulating attacks on one's own network or to train security teams (Rapid7, n.d.).

Patriotic hacking: Sometimes also referred to as nationalistic hacking. A group of individuals originating from a specific state engage in cyberattacks in defense against actors that they perceive to be enemies of their country (Denning, 2011, p. 178).

Ransomware: Malware that locks the user's computer system and would unlock it only when a ransom is paid (Trend Micro, 2017).

Remote Administration or Access Tool (RAT): Software granting remote access and control to a computer without having physical access to it. RAT can be legitimate software, but also malicious (Siciliano, 2015).

Script kiddies: Attackers who use cybertools that have been developed by more experienced and sophisticated hackers. Their main motive is to gain attention (PCtools, 2016).

Sender Policy Framework (SPF): Technical system validating email senders as coming from an authenticated connection in order to prevent email spoofing (Openspf, 2010).

Spear phishing: A sophisticated phishing technique that not only imitates legitimate webpages, but also selects potential targets and adapts malicious emails to them. Emails often look like they come from a colleague or a legitimate company (Ghernaouti-Hélie, 2013, p. 440).

SQL Injection: A cyberattack technique in which malicious code to be executed by a SQL server is injected into code lines (Microsoft, 2016).

Trojan horse: Malware hidden in a legitimate program in order to infect and hijack a system (Ghernaouti-Hélie, 2013, p. 441).

Watering hole attack: Attack where a legitimate website is injected with malicious code that redirects users to a compromised website which infects users accessing it (TechTarget, 2015).

Website defacement: Cyberattack replacing website pages or elements by other pages or elements (Ghernaouti-Hélie, 2013, p. 442).

10 Abbreviations

APT	Advanced Persistent Threat
BJP	Bharatiya Janata Party - India
C&C	Command and Control infrastructure
ISI	Inter-Services Intelligence - Pakistan
MCS	Mallu Cyber Soldiers - India
PCA	Pakistan Cyber Army
RAT	Remote Administration or Access Tool
SPF	Sender Policy Framework

11 Bibliography

Bajoria, J., 2010. Profile: Lashkar-e-Taiba (Army of the Pure) (a.k.a. Lashkar e-Tayyiba, Lashkar e-Toiba; Lashkar-i-Taiba) [WWW Document]. Counc. Foreign Relat. URL https://web.archive.org/web/20100605151918/http://www.cfr.org/publication/17882/ (accessed 11.04.18).

Balduzzi, M., Flores, R., Gu, L., Maggi, F., 2018. A Deep Dive into Defacement: How Geopolitical Events Trigger Web Attacks (TrendLabs Research Paper). Trend Micro.

BBC News, 2018a. Pakistan profile - Timeline [WWW Document]. BBC News. URL http://www.bbc.com/news/world-south-asia-12966786 (accessed 14.03.18).

BBC News, 2018b. India profile - Timeline [WWW Document]. BBC News. URL http://www.bbc.com/news/world-south-asia-12641776 (accessed 14.03.18).

BBC News, 2001. India-Pakistan: Troubled relations [WWW Document]. BBC News. URL http://news.bbc.co.uk/hi/english/static/in_depth/south_asia/2002/india_pakistan/timeline/default.stm (accessed 13.03.18).

BBC News, 1998. World: South Asia Indian army Website ambushed [WWW Document]. BBC News. URL http://news.bbc.co.uk/2/hi/south_asia/194844.stm (accessed 21.03.18).

Blaich, A., Flossman, M., 2018. Stealth Mango and Tangelo: Nation state mobile surveillanceware stealing data from military & government officials [WWW Document]. Lookout Blog. URL https://blog.lookout.com/stealth-mango (accessed 25.05.18).

Bussoletti, F., 2018. Between India-Pakistan is ongoing a cyberwar involving “patriot hackers” [WWW Document]. Difesa Sicurezza. URL https://www.difesaesicurezza.com/en/cyber-en/between-india-pakistan-is-ongoing-cyberwar-involving-patriot-hackers/ (accessed 21.03.18).

Center for Strategic and International Studies, 2018. Significant Cyber Incidents [WWW Document]. Cent. Strateg. Int. Stud. URL https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity (accessed 25.01.18).

Cimpanu, C., 2016a. SmeshApp Removed from Play Store Because Pakistan Used It to Spy on Indian Army [WWW Document]. Softpedia. URL

http://news.softpedia.com/news/smeshapp-removed-from-play-store-because-pakistan-used-it-to-spy-on-indian-army-501936.shtml (accessed 28.03.18).

Cimpanu, C., 2016b. Pakistani Hackers Deface Websites for Seven Indian Embassies, One Police Station [WWW Document]. Softpedia. URL http://news.softpedia.com/news/pakistani-hackers-deface-websites-for-seven-indian-embassy-one-police-station-505119.shtml (accessed 12.04.18).

Cimpanu, C., 2016c. Pakistan Resumes Cyber-Espionage Operations Against India [WWW Document]. Softpedia. URL http://news.softpedia.com/news/pakistani-resume-cyber-espionage-operations-against-india-504874.shtml (accessed 28.03.18).

Cimpanu, C., 2015. Indian Hackers Deface 125 Pakistani Websites as Payback for Mumbai 2008 Attacks [WWW Document]. Softpedia. URL http://news.softpedia.com/news/indian-hackers-deface-125-pakistani-websites-as-payback-for-mumbai-2008-attacks-496903.shtml (accessed 20.03.18).

Collins, S., McCombie, S., 2012. Stuxnet: the emergence of a new cyber weapon and its implications. J. Polic. Intell. Count. Terror. 7, 80–91. https://doi.org/10.1080/18335330.2012.653198

Command Five Pty Ltd, 2011. Advanced Persistent Threats: A Decade in Review.

Crowdstrike, 2016. 2015 Global Threat Report. CrowdStrike.

Cymmetria, 2016. Unveiling Patchwork - the copy-paste APT. Cymmetria Research.

Dawn.com, 2015. Pakistani hacker allegedly defaces India's NIT website: report [WWW Document]. Dawn. URL https://www.dawn.com/news/1192087 (accessed 21.03.18).

DellSecureWorks, 2014. Advanced Threat Protection with Dell SecureWorks Security Services. Dell Inc.

Denning, D.E., 2011. Cyber Conflict as an Emergent Social Phenomenon, in: Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications. Holt and Schell, pp. 170–186.

D'Mello, G., 2017. A Pakistani Group Hacked Into 10 Indian University Websites As Revenge Against Indian Hackers [WWW Document]. India Times. URL https://www.indiatimes.com/technology/news/a-pakistani-group-hacked-defaced-10-indian-university-websites-as-retaliation-against-indian-hackers-276456.html (accessed 21.03.18).

DNA Web Team, 2015. Indo-Pak Cyber War: Indian hackers deface Pakistani website [WWW Document]. DNA. URL http://www.dnaindia.com/india/report-indo-pak-cyber-war-indian-hackers-deface-pakistani-website-2131410 (accessed 12.04.18).

E Hacking News, 2014a. Indian Railways website hacked by Pakistan Haxors Crew [WWW Document]. E Hacking News. URL http://www.ehackingnews.com/2014/01/indian-railway-website-hacked-by.html (accessed 12.04.18).

E Hacking News, 2014b. Bihar BJP website hacked and defaced by Pakistani Hackers [WWW Document]. E Hacking News. URL http://www.ehackingnews.com/2014/04/bihar-bjp-website-hacked-and-defaced-by.html (accessed 12.04.18).

E Hacking News, 2014c. Official websites of Taj Mahal and Agra Fort hacked by Pakistani hackers [WWW Document]. E Hacking News. URL http://www.ehackingnews.com/2014/05/taj-mahal-agra-fort-websites-hacked.html (accessed 12.04.18).

E Hacking News, 2013a. Pakistan Ministry Education website hacked by Indian Hackers [WWW Document]. E Hacking News. URL http://www.ehackingnews.com/2013/07/pakistan-ministry-education-website.html (accessed 11.04.18).

E Hacking News, 2013b. Over 30 Rajasthan Government websites hacked by Pakistan Hacker "H4x0r HuSsY" [WWW Document]. E Hacking News. URL http://www.ehackingnews.com/2013/12/rajasthan-government-websites-hacked.html (accessed 11.04.18).

Fagerland, S., Kråkvik, M., Camp, J., Moran, N., 2013. Operation Hangover: Unveiling an Indian Cyberattack Infrastructure. Norman Shark AS and Shadowserver Foundation.

FIA, 2015. Official Website Of Passport Office Kolkata Hacked by Pakistani Hackers [WWW Document]. Indep. News Cover. Pak. URL https://www.incpak.com/world/official-website-of-passport-office-kolkata-hacked-by-pakistani-hackers/ (accessed 12.04.18).

FP Staff, 2016. After surgical strikes, Pakistani hackers attack Indian websites with profanities, claim "revenge" [WWW Document]. FirstPost. URL http://www.firstpost.com/india/surgical-strikes-aftermath-india-pakistan-engage-in-cyber-war-fare-various-indian-websites-hacked-3035162.html (accessed 21.03.18).

Garsein, A., 2012. Pakistan vs India: Who's the better hacker? [WWW Document]. Express Trib. Blogs. URL https://blogs.tribune.com.pk/story/13457/pak

istan-vs-india-whos-the-best-hacker/ (accessed 21.03.18).

Geers, K., Kindlund, D., Moran, N., Rachwald, R., 2014. World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks. FireEye Inc., Milpitas, CA.

Ghernaouti-Hélie, S., 2013. Cyberpower: crime, conflict and security in cyberspace, 1. ed. ed, Forensic sciences. EPFL Press, Lausanne.

Hashim, A., 2014. Timeline: India-Pakistan relations [WWW Document]. Al Jazeera. URL https://www.aljazeera.com/indepth/spotlight/kashmirtheforgottenconflict/2011/06/20116151113058224115.html (accessed 14.03.18).

HelpNetSecurity, 2018. Investigation uncovers Luminosity Link RAT distributors, victims are in the thousands [WWW Document]. HelpNetSecurity. URL https://www.helpnetsecurity.com/2018/02/05/luminosity-link-rat/ (accessed 12.04.18).

Huss, D., 2016. Operation Transparent Tribe Threat Insight. Proofpoint.

International Business Times, 2015. Exclusive: Who are "Mallu Cyber Soldiers" that hacked Pakistan websites [WWW Document]. Int. Bus. Times. URL https://www.ibtimes.co.in/exclusive-who-are-mallu-cyber-soldiers-that-hacked-pakistan-websites-648366 (accessed 11.04.18).

Internet Corporation For Assigned Names and Numbers, 2016. Glossary [WWW Document]. ICANN. URL https://www.icann.org/resources/pages/glossary-2014-02-03-en#i (accessed 04.11.16).

joji, T.P., 2013. Did Pakistan's ISI penetrate BSNL's systems? [WWW Document]. Livemint. URL https://www.livemint.com/Industry/ZoQivrvfFjfOJV74NGaW8K/Did-Pakistans-ISI-penetrate-BSNLs-systems.html (accessed 11.04.18).

Joshi, S., 2012. 112 government websites hacked in the last 3 months [WWW Document]. The Hindu. URL http://www.thehindu.com/sci-tech/technology/internet/112-government-websites-hacked-in-the-last-3-months/article2999836.ece (accessed 20.03.18).

Khan, L.A., 2014. Hitting back, Indian hackers deface Pakistani websites [WWW Document]. The Hindu. URL http://www.thehindu.com/sci-tech/technology/internet/hitting-back-indian-hackers-deface-pakistani-websites/article5630449.ece (accessed 11.04.18).

Kovacs, E., 2016. Pakistan APT Group Targets Indian Government [WWW Document]. SecurityWeek. URL https://www.securityweek.com/pakistan-apt-group-targets-indian-government (accessed 28.03.18).

Kovacs, E., 2014. Indian Public Health Engineering Department Targeted by Pakistani Hackers [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Indian-Public-Health-Engineering-Department-Targeted-by-Pakistani-Hackers-423623.shtml (accessed 12.04.18).

Kovacs, E., 2013a. Commemoration of 2008 Mumbai Attacks: Pakistani and Indian Sites Hacked [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Commemoration-of-2008-Mumbai-Attacks-Pakistani-and-Indian-Sites-Hacked-403870.shtml (accessed 20.03.18).

Kovacs, E., 2013b. Anonymous and ZHC Join Forces for OpKashmir, Several Websites Hacked [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Anonymous-and-ZHC-Join-Forces-for-OpKashmir-Several-Websites-Hacked-329726.shtml (accessed 11.04.18).

Kovacs, E., 2013c. Indian Hacker Leaks Admin Passwords for 35 Pakistani Government Sites [WWW Document]. Softpedia. URL http://news.softpedia.com/news/Indian-Hacker-Leaks-Admin-Passwords-for-35-Pakistani-Government-Sites-336734.shtml (accessed 11.04.18).

Kumar Jha, A., 2014. Indo-Pak Conflict rises up, Hackers on the way for a Cyber war!!! [WWW Document]. TechWorm. URL https://www.techworm.net/2014/10/indo-pak-cyber-war-in-offing.html (accessed 12.04.18).

Kumar, M., 2012. 30 Pakistan government Sites goes down ! [WWW Document]. Hacker News. URL https://thehackernews.com/2012/01/30-pakistan-government-sites-goes-down.html (accessed 11.04.18).

Kumar, M., 2011a. More than 100 Pakistani Government sites under malware attack [WWW Document]. Hacker News. URL https://thehackernews.com/2011/11/more-than-100-pakistani-government.html (accessed 11.04.18).

Kumar, M., 2011b. Cyber Cell Mumbai Websites hacked by Pakistani Hacker [WWW Document]. Hacker News. URL https://thehackernews.com/2011/10/cyber-cell-mumbai-websites-hacked-by.html (accessed 11.04.18).

Kumar, M., 2011c. Biggest Pakistan News site Dawn.com hacked by LuCkY [WWW Document]. Hacker News. URL https://thehackernews.com/2011/12/biggest-

pakistan-news-site-dawncom.html (accessed 11.04.18).
Levene, B., Grunzweig, J., Ash, B., 2018. Patchwork Continues to Deliver BADNEWS to the Indian Subcontinent [WWW Document]. Paloalto Netw. URL https://researchcenter.paloaltonetworks.com/2018/03/unit42-patchwork-continues-deliver-badnews-indian-subcontinent/ (accessed 12.04.18).
Leyden, J., 2010. Indian feds' site besmirched in tit-for-tat Pak hack attack [WWW Document]. The Register. URL https://www.theregister.co.uk/2010/12/06/pak_india_cyberwar/ (accessed 20.03.18).
Lin, H., 2012. Escalation Dynamics and Conflict Termination in Cyberspace. Strateg. Stud. Q. 6, 46–70.
Livemint, 2008. Indian, Pak hackers deface govt websites [WWW Document]. Livemint. URL https://www.livemint.com/Industry/plntcevqDrjZFGBsB3RHLI/Indian-Pak-hackers-deface-govt-websites.html (accessed 11.04.18).
Lookout, 2018. Stealth Mango & Tangelo Selling your fruits to nation state actors (Security Research Report). Lookout.
Lunghi, D., Horejsi, J., Pernet, C., 2017. Untangling the Patchwork Cyberespionage Group [WWW Document]. Trend Micro. URL https://blog.trendmicro.com/trendlabs-security-intelligence/untangling-the-patchwork-cyberespionage-group/ (accessed 29.03.18).
Majumder, S., 2001. Indian news sites hacked [WWW Document]. BBC News. URL http://news.bbc.co.uk/2/hi/south_asia/1617478.stm (accessed 21.03.18).
Maness, R.C., Valeriano, B., 2017. The Dyadic Cyber Incident and Dispute Data, Versions 1.5 Incidents only 20 jan.
Mehta, P., 2015. Websites of several Kolkata colleges hacked [WWW Document]. DNA. URL http://www.dnaindia.com/india/report-websites-of-several-kolkata-colleges-hacked-2140527 (accessed 12.04.18).
Microsoft, 2016. SQL Injection [WWW Document]. Microsoft TechNet. URL https://technet.microsoft.com/en-us/library/ms161953(v=SQL.105).aspx (accessed 29.11.16).
Mid Day, 2012. Indo-Pak cyber war on Jan 26 [WWW Document]. Day. URL https://archive.mid-day.com/news/2012/jan/280112-Indo-Pak-cyber-war-on-Jan-26.htm (accessed 11.04.18).
Monitoring Desk, 2017. India, Pakistan cyber war intensifies [WWW Document]. The News. URL https://www.thenews.com.pk/print/176619-India-Pakistan-cyber-war-intensifies (accessed 29.03.18).
Nayar, K.P., 2015. Lesson from Mongolia [WWW Document]. The Telegraph. URL https://www.telegraphindia.com/1150517/jsp/frontpage/story_20545.jsp (accessed 25.05.18).
Novetta, 2016. Operation Blockbuster: Unraveling the long thread of the Sony attack. Novetta, McLean,Virginia, USA.
O'Neill, P.H., 2018. Pakistani military leverages Facebook Messenger for wide-ranging spyware campaign [WWW Document]. Cyberscoop. URL https://www.cyberscoop.com/pakistani-military-spyware-stealth-mango-tangelo-lookout/ (accessed 25.05.18).
Openspf, 2010. Sender Policy Framework [WWW Document]. Send. Policy Framew. URL http://www.openspf.org/Introduction (accessed 03.01.17).
Paladion Networks, 2015. Website Defacement: Costs and Prevention [WWW Document]. Paladion. URL http://paladion.net/website-defacement-costs-and-prevention/ (accessed 24.01.17).
Passeri, P., 2015. 16-30 November 2015 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2015/12/07/16-30-november-2015-cyber-attacks-timeline/ (accessed 27.03.18).
Passeri, P., 2014a. 16-28 Feb 2014 cyber attacks timelines [WWW Document]. HACKMAGEDDON. URL https://paulsparrows.files.wordpress.com/2014/03/16-28-feb-2014-cyber-attacks-timelines1.png (accessed 12.04.18).
Passeri, P., 2014b. 1-15 May 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2014/05/27/1-15-may-2014-cyber-attacks-timeline/ (accessed 26.03.18).
Passeri, P., 2014c. 16-31 October 2014 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2014/11/03/16-31-october-2014-cyber-attacks-timeline/ (accessed 26.03.18).
Passeri, P., 2012. 16-30 September 2012 Cyber Attacks Timeline [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2012/10/04/16-30-september-2012-cyber-attacks-timeline/ (accessed 23.03.18).
Passeri, P., 2011a. October 2011 Cyber Attacks Timeline (Part I) [WWW Document]. HACKMAGEDDON. URL

https://www.hackmageddon.com/2011/10/16/october-2011-cyber-attacks-timeline-part-i/ (accessed 23.03.18).

Passeri, P., 2011b. December 2011 Cyber Attacks Timeline (Part I) [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2011/12/21/december-2011-cyber-attacks-timeline-part-i/ (accessed 23.03.18).

Passeri, P., 2011c. December 2011 Cyber Attacks Timeline (Part II) [WWW Document]. HACKMAGEDDON. URL https://www.hackmageddon.com/2011/12/30/december-2011-cyber-attacks-timeline-part-ii/ (accessed 23.03.18).

PCtools, 2016. What is a Script Kiddie? [WWW Document]. PCtools Symantec. URL http://www.pctools.com/security-news/script-kiddie/ (accessed 20.03.17).

Press Trust of India, 2016. Revenue Website Hacked By Suspected Pak-Based Groups [WWW Document]. New Delhi Telev. URL https://www.ndtv.com/india-news/revenue-website-hacked-by-suspected-pak-based-groups-1274768 (accessed 12.04.18).

Purani, A., 2016. How India-Pakistan hackers escalated cyber war post surgical strikes [WWW Document]. Dly. O. URL https://www.dailyo.in/politics/india-pakistan-war-cyber-security-national-green-tribunal-hackers/story/1/13367.html (accessed 21.03.18).

QinetiQ Ltd, 2014. Command & Control: Understanding, denying, detecting. QinetiQ Ltd.

Rapid7, n.d. Metasploit [WWW Document]. Rapid7. URL https://www.rapid7.com/products/metasploit/ (accessed 22.02.17).

RFSID, 2016. Hacktivism: India vs. Pakistan [WWW Document]. Rec. Future. URL https://www.recordedfuture.com/india-pakistan-cyber-rivalry/ (accessed 13.03.18).

Ribeiro, J., 2008. Feuding India, Pakistani hackers deface web sites [WWW Document]. Networkworld. URL https://www.networkworld.com/article/2270168/lan-wan/feuding-india--pakistani-hackers-deface-web-sites.html (accessed 20.03.18).

Sancho, D., Hacquebord, F., 2016. Operation C-Major: Information Theft Campaign Targets Military Personnel in India (TrendLabs Report). Trend Micro, Cupertino, CA, USA.

Settle, A., Griffin, N., Toro, A., 2016. Monsoon - Analysis of an APT Campaign (Special investigations). Forcepoint.

Sharma, M., 2013. India pins cyberattacks on Pakistani hackers [WWW Document]. ZDNet. URL https://www.zdnet.com/article/india-pins-cyberattacks-on-pakistani-hackers/ (accessed 11.04.18).

Shekhar, S., 2016a. Pro-Pakistan hacker on Intel agencies' watch, hacked more than 1,000 Indian websites [WWW Document]. India Today. URL https://www.indiatoday.in/mail-today/story/intel-agencies-track-pro-pakistan-hacker-afzal-faizal-who-hacked-thousands-of-indian-sites-333886-2016-08-08 (accessed 12.04.18).

Shekhar, S., 2016b. "Patriotic" Indian hackers lock Pakistani websites and refuse to give back the key [WWW Document]. Dly. Mail. URL http://www.dailymail.co.uk/indiahome/indianews/article-3825751/Patriotic-Indian-hackers-lock-Pakistani-websites-refuse-key.html (accessed 21.03.18).

Shekhar, S., 2015. Indian hackers deface Pakistani websites on 26/11 anniversary [WWW Document]. India Today. URL https://www.indiatoday.in/mail-today/story/indian-hackers-deface-pakistani-websites-on-26-11-anniversary-274558-2015-11-27 (accessed 20.03.18).

Shukla, P., 2017. India-Pakistan Gear Up For Cyber Wars This I-Day [WWW Document]. Businessworld. URL http://businessworld.in/article/India-Pakistan-Gear-Up-For-Cyber-Wars-This-I-Day/14-08-2017-124037/ (accessed 21.03.18).

Siciliano, R., 2015. What is a Remote Administration Tool (RAT)? [WWW Document]. McAfee Blog. URL https://securingtomorrow.mcafee.com/consumer/identity-protection/what-is-rat/ (accessed 04.11.16).

Symantec Security Response, 2013. Operation Hangover: Q&A on Attacks [WWW Document]. Symantec. URL https://www.symantec.com/connect/blogs/operation-hangover-qa-attacks (accessed 19.03.18).

TechTarget, 2015. watering hole attack [WWW Document]. TechTarget. URL http://searchsecurity.techtarget.com/definition/watering-hole-attack (accessed 29.11.16).

ThreatConnect Research Team, 2014. Debugging the Pakistan Cyber Army: From Pakbugs to Bitterbugs [WWW Document]. ThreatConnect. URL https://www.threatconnect.com/blog/debugging-pca-from-pakbugs-to-bitterbugs/ (accessed 19.03.18).

ThreatConnect Research Team, 2013. Where There is Smoke, There is Fire: South Asian Cyber Espionage Heats Up [WWW Document]. ThreatConnect. URL

https://www.threatconnect.com/where-there-is-smoke-there-is-fire-south-asian-cyber-espionage-heats-up/ (accessed 19.03.18).

TNM Staff, 2016. On Independence day, Kerala cyber Warriors hack 50 Pakistan websites [WWW Document]. News Minute. URL https://www.thenewsminute.com/article/independence-day-kerala-cyber-warriors-hack-50-pakistan-websites-48236 (accessed 11.04.18).

Trend Micro, 2017. Ransomware [WWW Document]. Trend Micro. URL https://www.trendmicro.com/vinfo/us/security/definition/ransomware (accessed 19.02.18).

Trivedi, S., 2016. Indian hackers launch massive cyber attack on Pakistan govt's network [WWW Document]. Deccan Chron. URL https://www.deccanchronicle.com/technology/in-other-news/071016/cyber-war-indian-hackers-lock-pakistans-data.html (accessed 21.03.18).

Vijay, 2015. Indian hackers pay homage to 26/11 Mumbai attack martyrs by hacking 200 Pakistani websites [WWW Document]. TechWorm. URL https://www.techworm.net/2015/11/indian-cyber-warriors-pay-homage-to-2611-martyrs-by-hacking-200.html (accessed 12.04.18).

Waqas, A., 2014a. Official website of Bangalore City Police hacked by Pakistani hacker [WWW Document]. HackRead. URL https://www.hackread.com/pakistani-hacker-hacks-bangalore-police-website/ (accessed 12.04.18).

Waqas, A., 2014b. India's Ludhiana City Rural Police Website Hacked by Pakistani Hackers [WWW Document]. HackRead. URL https://www.hackread.com/pakistani-hacker-hacked-india-police-website/ (accessed 12.04.18).

Waqas, A., 2013a. Free Kashmir Says Pakistani Hackers after Hacking and Defacing 20,000 Indian Websites [WWW Document]. HackRead. URL https://www.hackread.com/pakistani-hackers-hack-20k-indian-sites/ (accessed 11.04.18).

Waqas, A., 2013b. Official Website of Maharashtra Police Academy, India Defaced by Pak Cyber Pyrates [WWW Document]. HackRead. URL https://www.hackread.com/pcp-defaces-maharashtra-police-academy-website/ (accessed 11.04.18).

Web Desk, 2014a. Suspected Indian hackers deface Pakistan's MET website [WWW Document]. Express Trib. URL https://tribune.com.pk/story/797390/suspected-indian-hackers-deface-pakistans-met-website/ (accessed 20.03.18).

Web Desk, 2014b. Indian hackers deface PPP website in response to Bilawal comments [WWW Document]. Express Trib. URL https://tribune.com.pk/story/772218/indian-hackers-deface-ppp-website-in-response-to-bilawal-comments/ (accessed 20.03.18).

Web Desk, 2014c. 22 Indian government websites hacked by Pakistani hackers [WWW Document]. Express Trib. URL https://tribune.com.pk/story/787766/22-indian-government-websites-hacked-by-pakistani-hackers/ (accessed 20.03.18).

Wei, W., 2013. Unofficial Pakistan Intelligence website hacked [WWW Document]. Hacker News. URL https://thehackernews.com/2013/03/pakistan-intelligence-agency-hacked-by.html (accessed 11.04.18).

Windows Defender, 2011. Backdoor:Win32/Bezigate.B [WWW Document]. Window Def. URL https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Backdoor:Win32/Bezigate.B&ThreatID=-2147289544 (accessed 12.04.18).

Xu, E., Guo, G., 2018. Hacking Group Spies on Android Users in India Using PoriewSpy [WWW Document]. TrendMicro. URL https://blog.trendmicro.com/trendlabs-security-intelligence/hacking-group-spies-android-users-india-using-poriewspy/ (accessed 28.03.18).

CSS
ETH Zurich

The **Center for Security Studies (CSS) at ETH Zurich** is a center of competence for Swiss and international security policy. It offers security policy expertise in research, teaching and consulting. The CSS promotes understanding of security policy challenges as a contribution to a more peaceful world. Its work is independent, practice-relevant, and based on a sound academic footing.