Citation: Anwar, S. S., & Yamin, T. (2021). Civil Military Cooperation (CIMIC) in Cyber Security Domain: Analyzing Pakistan's Prospects. *Global Strategic & Security Studies Review, VI*(I), 68-81. https://doi.org/10.31703/gsssr.2021(VI-I).08

DOI: 10.31703/gsssr.2021(VI-I).08 **p- ISSN:** 2708-2121 **e-ISSN:** 2708-3616 **L- ISSN:** 2708-2121

Civil Military Cooperation (CIMIC) in Cyber Security Domain: Analyzing Pakistan's Prospects

Pages: 68 – 81 | **Vol.** VI, **No.** I (Winter 2021) | **URL:** http://dx.doi.org/10.31703/gsssr.2021(VI-I).08

Syeda Sundus Anwar * | Tughral Yamin †

Abstract *A clear lack of Civil-Military Cooperation is evident in the field of national cybersecurity policy. For a country such as Pakistan with fractious political, cultural, and diverse ethnic identities and ideological characteristics, an unguarded cyber domain can add to the existing rifts. In light of these challenges, Pakistan needs to create a national cybersecurity policy and strategy incorporating both civil and military concerns. The aim of this research paper is to find out a conceptual framework of Civil-Military Cooperation (CIMIC) in the realm of cybersecurity. This study has used open-ended semi-structured interviews to find out the way forward and the hindrances in civil-military cooperation to create a robust national cybersecurity regime. For an effective national cybersecurity policy, synergy has to be created between the civil and military sectors. The military should not only have the necessary cybersecurity expertise, but it should also organize cyber-drills incorporating all stakeholders.*

Key Words: CIMIC, Cybersecurity, Cyberwarfare, Synergy, Trust

Introduction

Technological advances in cyberspace have redefined relations among states and institutions within the state. It has resulted in unprecedented security challenges. Globally, the importance of resilience in cybersecurity cannot be overemphasized (Lipton, 2020). Technologically advanced countries have taken due cognizance of it to ensure the safety and security of their economies, health services, and internal and external defense.

For a country such as Pakistan, with fractious political, culture, diverse ethnic identities, and ideological characteristics, an unguarded cyber domain can add to the existing rifts that can impact civil-military cooperation (CIMIC). In a report released by Comparitech (2019), a UK based pro-consumer website, Pakistan is ranked 7th worst in terms of cybersecurity. This assessment is based on seven indicators:

- Percentage of mobiles infected by malware;
- Financial malware attacks;
- Percentage of computers infected with malware;
- Percentage of telnet attacks by originating country;
- Percentage of crypto miners (software developed for the purpose of taking over a user's computer and using it without the user's knowledge or permission to mine currency);
- Best prepared for cyberattacks and most up-to-date legislation.

* MS Scholar, Department of Peace and Conflict Studies, National University of Science and Technology (NUST), Islamabad, Pakistan. Email: sundus.anwar28@gmail.com
† Associate Dean, Centre for International Peace & Stability (CIPS), National University of Science and Technology (NUST), Islamabad, Pakistan.

Pakistan's adoption of cybersecurity practices requires the implementation of a national cybersecurity policy to help create an environment of cooperation between the military and civil leadership in the cyber domain. It will direct both institutions to carefully deal with the vulnerabilities created in the social media domain and deal with each other in a friction-free environment.

In this paper, an effort has been made to examine the applicability of the conceptual framework of Civil-Military Cooperation (CIMIC) in the national cybersecurity domain. Pakistan lacks a cybersecurity strategy; therefore, any cooperation with regional or international actors in the domain lacks the vision of operational and tactical level implementation. This paper addresses the hurdles in creating a common national cybersecurity strategy incorporating both civil and military concerns; the vulnerabilities that lead to unsafe national cybersecurity domains in Pakistan. The paper also analyses the prospective areas of cooperation between both actors. The Prevention of Electronic Crime Act (2016) set out provision for international cooperation in Chapter IV, section 39 on International Cooperation. However, due to the lack of a national CERT, National Cyber Security Strategy and implementation of cybersecurity policy, Pakistan has not been able to secure its own cyberspace.

This means, among other things, that Pakistan needs a national cybersecurity strategy to develop a framework that encourages cybersecurity cooperation among state organs and other states. A CIMIC architecture in cybersecurity based on multi-stakeholder engagement could provide a better understanding of the vulnerabilities in cyberspace. This paper shall make an attempt to highlight and analyze major hindrances in policy-making related to cybersecurity, key areas of collaboration between civil-military organizations and a prospective roadmap to meet international standards.

Existing secondary sources such as books, newspaper articles, national and international policy documents, working papers, research articles, Tallinn Manual 2.0, Prevention of Electronic Manual (2016) have been consulted as part of the research. To address the issues discussed in this paper and formulate a way forward, semi-structured interviews were conducted with ten cybersecurity experts, four from the military sector and six from the civil sector. Most of the interviews were conducted via zoom, given the current pandemic. The respondents were selected on the basis of their years of experience in Pakistan's cybersecurity domain, their cross-sectoral experience, and exposure to the civil-military sector simultaneously. Empirical data has been collected via field research to better formulate a coordinated responses to the rising cybersecurity issues in the country and Pakistan's role in Cyber Security CIMIC.

Cybersecurity in Pakistan

Cyber threat intelligence requires broad-based collaboration, where no institution works in a standalone mode. Pakistan's National Internal Security Policy (NISP) has addressed the issue of cyber threats and underscored the need for a civil-military command for inter and intra agency coordination (NISP, 2018). To date, neither a civil-military command nor a common national cybersecurity strategy has been implemented. Additionally, the policy paper does not discuss the international cooperation to adopt best practices and secure Pakistan's cyberspace. A policy gap remains that needs to be addressed by the Pakistani academia, political leadership, bureaucratic leadership and the military for a holistic and air-tight national cyber policy. This gap has been identified by Rubab Syed et al (2019). The need for interagency contingency plans, according to Jensen and Work (2018), cannot be ignored. Therefore, Pakistan should not only prepare itself against physical external and internal attacks, but it should also have robust cyber defences against virtual attacks on its critical infrastructure (ibid).

Neighboring countries such as India and Bangladesh have been allocating budget and manpower to the IT sector, including collaboration between the civil and military sectors in cyberspace for a coordinated response (Policy, 2013). Understanding the cyber posture of both states and non-state actors has become a prerequisite for all foreign and domestic policy standings (Salmaan, 2018). This assumes importance as society shifts to

cyberspace to conduct all sorts of businesses (Firdous, 2018).

A comprehensive response plan (CRP), as recommended in the NISP (2014-18), requires a strong CIMIC framework (NISP, 2014). The security of national cyberspace needs prompt preemptive joint civil and military measures. Hassan (2019) mentioned the ITU wellness report to improve cybersecurity health and Pakistan lack of certified national Cyber Emergency Response Team (CERT) hindering development and increasing insecurity vis-a-vis cyberspace.

Yamin (2014) recommends confidence-building measures (CBM) in cybersecurity between Pakistan and India to build robust cybersecurity at the bilateral level. Such practices can be extended to include other regional and extra-regional actors through CIMIC. Yamin (2018) proposed raising the issue of regional cooperation in cybersecurity on the forum of the Shanghai Cooperation Organization (SCO) by Pakistan's foreign office.

Syed et al. (2018) emphasize inter-sectorial coordination between different public-private and military institutions. Writing further, that the public sector vulnerability to cyber-attacks in the form of credit card frauds, phishing, spamming and extraction of other financial information can bring the economy of a country down to its knees.

Therefore, it cannot be ignored that the military sector faces security challenges in case the critical public infrastructure of the country is targeted. According to an article published in *Express Tribune* (2016), referring to the Intercept, National Security Agency (NSA) reportedly spied on Pakistan's civil and military leadership using an NSA software called 'SECONDATE'. Pakistan Navy (PN) was targeted using the 'target collision hijacking method' through malware 'rattlesnake', specifically targeting the PN's Public Relations Bureau (Khalil, 2020). Vombatkere (2018), in the context of India, mentioned the implications of hardware and software as they are foreign technologies bought in foreign markets. The hardware and software 'target the defense, home, finance and banking operations, energy including oil .... Electric power, nuclear power...air traffic control...', 'public or private sector industry including Unique Identification Authority of India's (UIDAI) Central ID Repository (CIDR)', (ibid). This presents a unique question for militaries and civilian leaderships of any country as they adopt policies on cyberspace in standalone capacity minimizing the role of a collaborative effort.

The Niche of CIMIC in Cybersecurity in Pakistan

Cybersecurity and CIMIC

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks (Kaspersky, 2020). ITU (2020) defines cybersecurity as:

> The collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Bruan (2005) described the concept of CIMIC as a Collective term for all kinds of interactions between civilian organization, including individual national and international bodies with the deployed military forces.

Within NATO, CIMIC is a military function comprising a set of capabilities to accomplish missions and help commanders to establish effective civil-military interaction with other non-military actors. According to the NATO CIMIC Doctrine (Allied Joint Doctrine for Civil-Military Cooperation - AJP-3.4.9), CIMIC is The coordination and cooperation, in support of the mission, between the NATO Commander and civil actors, including national population and local authorities, as well as international, national and non-governmental organizations and agencies (2018).

Though military oversight exists in cybersecurity, the practical application of CIMIC in the field of cybersecurity is still in the early stages.

The impact of technology, as discussed in the AJP3.19 (2018) NATO CIMIC document, is a key strategic driver among other threat vectors. In the section covering CIMIC support in the cyberspace environment, early operational situational awareness in cyberspace has been emphasized due to increasing cyberattacks.

According to AJP 3.19 (2018): 'the contemporary operating environment includes a myriad of ethnic, religious, ideological issues.' These issues also include 'technological issues. Requiring:

> Sustainable solutions in societies disrupted by conflicts. Solutions to these serious events are impossible to achieve by military means alone. (AJP 3.19, 2018)

NATO allies at Warsaw 2016 summit recognized cyberspace as a 'domain of operations' similar to air, land and sea, where the organization must protect itself (Cyberdefense policy, 2020). Heinl (2015), in the policy report, addresses the gap within organizational structures in the EU and Asia and their military cyber defence. Heinl (p.5, 2015) refers to the military cyber defence in EU and Asia as 'in the early stage of maturity.'

In cyberspace, demarcations between civil-military sectors are more or less defined. Understanding the aspect related to the security of cyberspace also requires a multiple-stakeholder approach to defend against external and internal threats, especially against the critical infrastructure of a country. Critical infrastructure has been defined as (T)the body of systems, networks and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety(target,2020).

Most cyber-related issues do not adhere to the traditional crisis mode and can occur unexpectedly. The Wannacry malware presents a case that has proven the silent destructive nature of the cyberattack, causing substantial financial losses. Thus, a need for peacetime emergency planning is important to ensure safety in cyberspace.

Pakistan civil infrastructure, public-private and military actors, have also been targets of cyberattacks. In 2020, the Karachi Electric power grid was a target of ransomware (Dawn, 2020). In August 2020, Indian Intelligence attacked civil and military personnel's personal mobile and information gadgets (Tribune, 2020). In 2018, 22 Pakistani banks' card holder's data was put on sale on the dark web (Dawn, 2018). However, Pakistan has been unable to implement a cybersecurity strategy and cybersecurity policy. Moreover, for any international cooperation against cybercrime, there is a need for ratification Budapest Convention on Cybercrime which Pakistan is not a signatory to.

CIMIC and Cybersecurity: Case of Pakistan

A cyberattack could 'contribute towards a state collapse, in case of initiating or prolonging failure of critical national infrastructure' (Robinson et al., 2018). Pakistan's military intelligence has a sophisticated cybersecurity architecture and cyber-surveillance system (International, 2015); however, a broad-spectrum cybersecurity policy covering health, economics, critical infrastructure and counter-terrorism aspects is also needed. According to Information Telecommunication Union (ITU) (2018) report, 103 countries in the world have National Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRT). The functions of these teams are to provide aid to corporations, enterprises and nations in case of cybersecurity incidents. Making them an important component of cybersecurity defense where civil and military sectors can cooperate (access, 2020). In Pakistan, there are some organizations where civil-military information security experts are working together, such as Special Communication Organization (SCO). Pakistan's National Response Center for Cybercrime (NR3C) mixes CERTs from both the civil and military sector for a more holistic response. The concentration, however, is more in the security sector.

In Pakistan, the institutions in charge of cybersecurity matters are the National Response Center for Cyber Crime (NR3C), National Center for Cyber Security (NCCS) and Ministry for information and technology (MoIT). The importance of these institutions in light of the lack of civil-military cooperation in the cybersecurity domain becomes more defined. The gaps that exist in Pakistan's cybersecurity between the civil and military organizations can have implications for the state itself and its relations with other regional and extra-regional countries. The presence of a niche in cybersecurity in Pakistan in the form of policy documents, yet not legislated, has left

the country with weak cybersecurity practices. Moreover, there is a lack of governance in cybersecurity, and the civil-military sectors have relied on self-governance in cybersecurity.

Pakistan has established the National Center for Cyber Security (NCCS, 2018), but this lacks the capacity for emergency planning and execution of a plan during a crisis. The Center has the representation of both civil and military but has yet not been fully operational.

According to digital Pakistan (2020), the total number of internet users in January of 2020 was recorded at 76.38 million, which makes it a 35percent of the population. As the number of users increase, so does the vulnerability and cyber insecurity. In 2016 Pakistan's Parliament passed Prevention Electronic Crime Acts (PECA); however, the bill faced resistance from private and digital activists for the 'impact of legitimate business and citizens rights' (Bolobhi, 2015). In 2019, law enforcement agencies surveilled the footage of the student solidarity march and registered cases against the participants (The News, 2019). The country's intelligence agency had been carrying mass network surveillance since 2005 of apex court judges, politicians' activists, lawyers and journalists (Dawn, 2017). Such practices by the state agencies have created mutual distrust, and private actors and the civilian sector show reservations in cooperation.

Considering such reservations by private and public sectors, a council for mutual participation needs to be formulated. One such council in dealing with multi-stakeholders was the National Security Council (NSC). NSC Pakistan consisted of multiple stakeholders to help the country deal with different policy issues (Ali, 2015). In the case of cybersecurity, such a council does not exist.

In 2018, former National Security Advisor (NSA) Lt Gen Nasser Khan Janjua (retd) emphasized the need to focus on non-traditional threats to hitherto unexplored areas such as cybersecurity (Jabri, 2018). The multifaceted cybersecurity threats include malware attacks, cyberespionage, cyber theft, identity theft and Distributed Denial of Service (DDoS) (Rafiq, 2019). These threats are to both civil and military sectors. Even though the nature of the attacks and policy gaps are identified, and institutions such as NR3C deal with cybercrimes under FIA, the concentration is on resolving the crimes that are reported, not broader aspects of cooperation and securing the country's cyber gateways.

Asia Center note (2018) coined the term 'cyber-enabled information conflict' that can cause equally grave consequences as a physical conflict in a borderland. According to the note (2018), 'cyber-enabled information conflicts are increasingly shaping the character of regional security flashpoints…' resultantly tensions can escalate between adversaries. According to Fravel (2015), who quoted from China's Defense White Paper, 2015 'the form of war is accelerating its transformation to informatization.' It could also escalate the internal threat vector of a state, as there exists resentment between different institutions and the public. According to the 2013 Wikileaks, the boundless informant heatmap (Greenwald and MacAskill, (2013) showed Pakistan as one of the most surveilled countries by NSA. Both civil-military actors were targeted. The attacks and practices in cyberspace do not end only with surveillance. Countries collect the data for information purposes and generating 5th generation warfare. Pakistan, due to multiple threats of sectarian violence, terrorism, ethnic and religious divisions and poor economic development, is more vulnerable.

According to the Global Security Index report, Pakistan has shown a commitment to cybersecurity programs and initiatives (GCSI, 2018). However, Pakistan needs to develop step by step approach to making its neighborhood safe from cyberattacks while formulating interregional cooperation. This can also help in better CIMIC policies in cybersecurity as Pakistan is one of the most surveilled countries in the world (International, 2015). In 2019, senior official cellphones were hacked via Whatsapp for 'covert surveillance (Qadeer, 2020). Pakistan, by developing a national cybersecurity strategy, can be better prepared in the future to deal with increasing cyberattacks.

Lack of indigenization of technology creates vulnerability for cybersecurity in Pakistan. Lack of information sharing between government sectors and the military sectors can lead to future security breaches and disinformation between the two sides. All

these issues arise from poor governance of cybersecurity. The dual-use technology leaves civilian institutions more vulnerable; at the same time make them the last line of defence in the domain of cybersecurity.

Lack of policy also results in a lack of an overarching body, where CIMIC can take place in a cordial atmosphere. Yamin (2018) pointed towards the absence of a central body that could coordinate the cybersecurity ecosystem, provide advice to the Prime Minister on Cyber threats. There is also private actors' reluctance to cooperate with the civil-military sector due to breach of basic human rights—a consequence of weak good governance practices of the country and lack of institutional response. Throughout the globe, civic societies, military and government sectors are realizing the impact of cybersecurity on national security; however, Pakistan has a long way to go. In the next section of data analyses, the gaps in Pakistan's cybersecurity has been analyzed. This provides us lead on how these gaps can be mitigated.

Data Analysis

Pakistan has been unable to bring together its military and civilian stakeholders when the National Cybersecurity council Bill (NCSC) was proposed in the senate in 2014. This has enhanced the cybersecurity vulnerability of the country.

CIMIC in Correlation with Policy in Pakistan

Interviews from local cybersecurity experts have resulted in some interesting insights (all interviews were held in confidentiality, names have been withheld). Respondents generally agreed that the dependency of a state on technology had elevated the vulnerability of cyberspace. Additionally, the lack of cybersecurity surpasses the threat of weapons of mass destruction. Experts unanimously agreed that policy holds utmost significance in defining the role of a nation and where it stands. In 2014, all stakeholders came together to formulate National Cybersecurity Council Bill (2014); however, the bill is still pending in the senate. Lack of CSITRT and a national CERT, along with disintegrated military and civilian sectors responses, hinders progress in the domain (Expert G, 22 August 2020). The military preparedness for any unprecedented cyber event within Pakistan does exist, but the civil side remains vulnerable. The hindrance that exists in Pakistan's cybersecurity is that our cybercrime bill does not have any provisions of cybersecurity even though both are interlinked.

On the military side, there are reservations in cooperating with the civil side. As one respondent argued, 'that the sectors are isolated'. While another respondent stated

'CIMIC is not possible in the near future due to trust deficit. The military is an isolated network. The military has its own setup in place, which is based on an 'airgap' network". Another factor for the military's reluctance for cooperation is the lack of expertise in the civil side. 'A lack of balance in capabilities between the civil and military hinders chances for cooperation. The civilians have traditional networks, where the knowledge is public domain' (Expert I, 19 August 2020). However, the challenge is that cyberspace is for operational purposes in the civil infrastructure, such as dams, water, roads, power grids, power plants and airways. As the fifth domain of warfare and a global common, the military cannot work in isolation despite a separate secure network. The lack of CIMIC in cybersecurity also results in economic hindrances. One of the experts mentioned that 'our poor cyber defences in the banking sector has resulted in the loss of USD 6 billion dollars in 2018 alone.' Due to weak data protection and lack of capabilities, we are unable to bring stakeholders, resultantly affecting our knowledge economy.

Experts were of the opinion that Pakistan neither has a well-developed cybersecurity policy nor cyber diplomacy. On research, through different platforms, it was found that it is due to the power struggle between the stakeholders in the domain. The military considers cybersecurity in the perspective of warfare alone. While the civil perspective revolves around particular strands of cybercrime, including harassment, hacking, cyberbullying. The consideration for the connection of cybercrimes to greater threats such as malware attacks, ransomware attacks or attacks on critical infrastructure is not covered under the anti-cybercrime practices. According to one expert, 'on the importance of cybersecurity experts in post-conflict scenario:

'military considers cybersecurity to be a military domain' (Expert I, 19 August 2020). Another expert emphasized that 'the military should let the civilian side work (Expert D, 22 August 2020). Most of the experts almost shared the view that the domain of cybersecurity needs 'well-developed infrastructure.' To strengthen this area, civil-military cooperation is required that needs a good policy in order to handle security, enhanced and implemented at a higher level.

The importance of civil cyber experts has been emphasized by the experts. According to one expert, 'more is less.' In the view of another expert, they ensure the availability of cybersecurity to the masses and the military. One respondent revealed that 'research and development skills are available and Pakistan's civilian side is more equipped with cyber capabilities than the military (Expert F, 23 August 2020),' which could help in sharing knowledge of the civilian environment with the military sector and equipping it for unforeseen scenarios in the cyberspace.

Experts have highlighted the need for the identification of experts within civil and private institutions for preparedness in the cybersecurity domain. There are a number of institutions within civil and military sectors that have representation of cyber-experts in both sectors; however, the forces still need civil-cyber functional experts, who through training and exercises could help in providing the first line of defence for the country.

According to a respondent ' the military complex has dependencies from an information highway perspective, including logistics such as water, roads and dams (Expert C, 19 August 2020). Even though the military aims to gain a digital high ground, both military and civil cybersecurity are intertwined. The security of the military cannot be ensured if they do not extend expertise to their civil counterpart in an organizational capacity.

A few experts emphasized the importance of awareness in the domain of cybersecurity. Awareness will be created vis-à-vis the cybersecurity policy devised. This will lead to cooperation between the two sectors.' Cyberspace intertwines and is an intersection of economies. It is very important for that purpose to manage military and non-military relations.

Need for Synergy in Cyber Security

Along with the military, we need civil professionals who can promptly deliver results. There is a need for a well-devised road map towards cybersecurity. Support for cyber CERTs lacks on both the civil and military side, resulting in the private PAK-CERTs organizations participation in an unofficial capacity in the international cyber drills. In cyber drills 'military takes part in an unofficial capacity (Expert G, 21 August 2020), weakening cooperation through shared platforms in an official capacity. Moreover, we 'lack the indigenization of technology and awareness. There is also a lack of formalized assessment (Expert D, 22 August 2020).

According to a number of respondents, if there is a cyberattack launched from Pakistan's soil on a third party, Pakistan will be unable to respond to whether Pakistan's cyberspace was compromised or it was involved in the attacks. Due to a lack of trust on the military side, there could be a delay in information sharing in case of a cyberattack. As one of the respondents elaborated, 'if there is an incident Pakistan response will suffer, and lack of capability further hinders the response. It springs from a lack of awareness and policy. Resultantly no response to the attack will take place due to lack of detection' (Expert I, 19 August 2020). The issue also arises in citizen privacy. Some experts deemed it necessary for the law enforcement agencies and the military establishment to monitor cyberspace. On the question of ensuring the human rights of the private actors, how synergy can be created between civil-military and private actors, one respondent emphatically put 'there is no personal security above Pakistan. Personal information does not matter' (Expert H, 24 August 2020). Another respondent argued that 'sometimes people do not understand why interception of data and security is important, but it is definitely important if it is used for the right purposes' (Expert F, 24 August 2020). Such mindsets detract a country's path towards growth in the cybersecurity sector.

Joint civil-military exercises are required within a robust cybersecurity plan to bridge the

gap between Pakistan and the rest of the world. CERTs are needed to be integrated at all levels, which requires joint exercises. Military needs to take part in cyber drills organized by private actors. Through these exercises, a synergy can be created between civil-military within Pakistan. Further, the indigenization of the country's firewalls, its technologies in the public sector could boost the confidence of the other sectors. It could help in avoiding any backdoors into our cyberspace and in building trust between the stakeholders.

According to one expert, cybersecurity should be placed under the National Security Division (NSD). Another expert mentioned 'there is a need for a figurehead that works directly under the President and Prime minister.' According to some respondents, 'Federal Investigation Agency (FIA) is mixing CERT from both military and civil' despite the lack of national CERT. A respondent also informed that in case of a 'bug, security flaw, or an attack Pakistan Telecommunication Authority (PTA) floats information' about it that is then shared between different individual setup, stating that 'cooperation is definitely there' (Expert F, 24 August 2020).

An initiative that is already in place in an unofficial capacity is the Cybersecurity Alliance of Pakistan (CSAP), by formalizing this alliance, Pakistan will have a starting point under which framework could be formalized. Under the framework, policy and strategy could be formulated, and assessments could be made based on certain checks and balances. The assessment will help formulate policies that will also ensure that it caters to the contours of the domestic setup while 'taking guidelines from the international policies', (Expert G).

One expert emphasized 'the need to form a form a National Cybersecurity Taskforce comprising civil and military experts to strengthen the cyberspace without compromising any civil rights.' EU has put in place the General Data Protection (GDPR) for the protection of individual rights in cyberspace. Similarly, there is California Privacy Act. Pakistan has introduced earlier this year the 'Citizens Protection against Harm Rule' and has in draft phase the 'Personal Data Protection Regulation of Pakistan (PDPR)'. The current laws are for cybercrimes in the country and do not cover cybersecurity. Cybersecurity laws could be an extension of the cybercrime bill. A council for mutual participation needs to be formulated specifically catering to the cybersecurity demands. The functions of this council should be separate from the National Response Center for Cyber Crime (NR3C).

Alliances and Cooperation

The civil-military actors come together both in an official and unofficial setting, as in the case of the Cybersecurity Alliance of Pakistan (CSAP). Officers from NESCOM, C4I, Airforce are part of Cyber Security Alliance of Pakistan (CSAP) drills, but not in an organizational capacity. The question arises who will lead the domain of cybersecurity in the case of international operation. As one respondent stated, 'invitations may come to either Ministry of Information Technology or to military, they may or may not share with the other side, as civil and military are not on the same page (Expert D, 22 August 2020). It also shows there is a trust deficit, even though both sides have capabilities. According to Expert A (8 August 2020), 'the inclination of the military is towards their own assets'. The standalone nature of the military cannot be fruitful when the attack is on the civil infrastructure.

According to Expert G (21 August 2020), heading the Cyber Security Alliance of Pakistan (CSAP), there are more than 'five hundred' members in the alliance.' The group members are from civil, army, CSOs and CISOs; these are also the people that are handling emergencies within Pakistan currently.

Providing support to non-military actors, developing their capacity, and information sharing could help in the capability and capacity building in the cybersecurity domain. Sending 'a message' to the world, as emphasized by one of the experts that, both sides are working together.

Next-generation is likely to see cybersecurity soldiers for that purpose; both civil and military cooperation is required. The state-owned policy is important for national and international alliances. NATO holds regular joint exercises. Therefore, it is an important aspect to collaborate in cybersecurity with the countries with whom Pakistan has friendly ties. The civilian side is more well versed in on-

ground day to day cyber realities, while the military's concentration is more on developing the offensive and defensive capabilities.

Federal Investigation Agency (FIA) coordinates with Interpol. A cyber investigation setup is in place that tracks down the suspects in collaboration with other countries. Pakistan has also taken part in cyber drills for the last twelve years. However, 'it is only the civilians that take part in these drills from the platform of PISA-CERT' (Expert G, 21 August 2020).

Needless to say, the overarching hindrance in Pakistan's cybersecurity is due to the political tug of war between the institutions. Similar to every other domain, cybersecurity in Pakistan has also been subjected to a lack of bureaucratic and political will. Additionally, there is reluctance in implementing a cybersecurity policy, despite the development of a framework for cybersecurity. Pakistan is marred with self-governance in cybersecurity, where, where-withal cybersecurity framework is not being developed.

A structured approach is needed in the Pakistan Cybersecurity domain. It could provide security during everyday measures, as part of developing policies, doctrine and concepts. Moreover, it could provide a road map for joint capability building and capacity building wherein the civilian sector will be at the forefront. As part of the capability component, an understanding and will to use the doctrine and concepts could also be developed through joint civil-military drills through the platforms such as PISA.

The gaps and mistrust within Pakistan's cybersecurity between the civil and military organizations, can create hindrances for the state itself, which requires incentives for cooperation, as discussed in the succeeding section.

Incentives for Cooperation

In order for the civil-military sector to cooperate, this study suggests:

Better Flow of Communication

Communication lines between civil and military sectors need to be open to reduce the trust deficit. The information must be reliable and authentic. A monthly panel discussion should take place where information is exchanged and updated. Once the military and civil sides have compatible capabilities, cooperation will follow. Civil-military cooperation in cybersecurity requires understanding the structures on both sides and need-based interference in the other sector. There is a need for coordination between different departments on immediate and non-immediate threats in the cybersecurity matrix. For this purpose, interagency cooperation as part of the comprehensive approach can be referred to. After the cyber-attack on Estonia's national infrastructure, the country adopted interagency cooperation under a comprehensive approach (Pernik, 2014). The data analysis section has specified the importance of cyber drills, exercised under interagency cooperation.

Institution Formation and Political Actors' Involvement

An organization in this wake needs to be formulated with researchers and policy advisors from both Civil and military sides. Based on the consensus developed, a way forward must be adopted. Sitting government and political actors must be involved to understand the constitutional deficit within the laws. It is suggested to involve political actors with knowledge of cybersecurity for establishing momentum of dialogue. It will help in streamlining the issues of the actors involvedand provide more clout to the governance in cybersecurity.

To address the inhibitions, lawful steps already identified under the constitution should be referred to. Inhibitions within cybersecurity between the civil-military sector could be resolve through constitutional and judicial means. The institutions must avoid extra-judicial and extra-constitutional means for cooperation. Lessons can be learnt from cybersecurity governance and the information security governance model from around the globe.

The cybersecurity governance model should be cost-affective. Understandable formats for civilian institutions could be

developed, especially for the law enforcement agency.

Legislative Reforms/Amendments

Our legislative bodies require experts on information technology and security. Incentives for cooperation require expertise on equal footing. For better cooperation, cybersecurity provisions need to be made part of the cybercrime bill. As the nature of cybercrimes, from malware to ransomware, could have a direct effect on the cybersecurity of a state. For cooperation between institutions, it is suggested, cooperation be mandated in cybersecurity. For interagency cooperation, the Agreement on cooperation among the member states of the Common Wealth of Independent States in combating offences relating to computer information article (5) (2008), the United States Sarbanes-Oxley Act (2002) mandating reporting requirements, NATO National Cyber Security Strategy Guidelines (2013) and Guide to developing a National Cybersecurity Strategy-ITU (2018) good practices can be consulted. It is suggested that institutionalized cooperation between private-civil-military sectors is promoted through the introduction of a generalized data governance model. Under the cybercrime bill, information sharing could be mandated to mitigate trust deficit and secure the country in case of cyberattacks.

The drafted cybersecurity policy must be revised for its deficiencies. The public sector needs to be involved and informed about the lawful surveillance by law enforcement agencies. Remaining within the constitution, citizen reservations on laws must be addressed. Article 7 General Data Protection Regulation (GDPR, 2016) on Conditions on consent could be referred to for guidance purposes.

Through the inclusion of CIMIC, Pakistan can approach the cybersecurity issue in Pakistan and South Asia from a broader perspective. It will also help in creating cyber defences of the country where both actors will be involved. Research needs to be broadened on civil-military cooperation in the components of information technology. Research Gap exist in information security governance in Pakistan. Further research could also be carried out in civil-military cooperation in information security.

Conclusion

There is no gainsaying the fact that CIMIC in cybersecurity is of primary importance. This study has identified some themes that could help in more productive CIMIC. The first step is to ensure that the civil-military sectors put their differences aside. Once institutional biases have been shed, much-needed synergy in cybersecurity can be created.

The country is facing losses due to vulnerability in its cyberspace through website defacement, phishing, attacks on government networks and cyberespionage. Lack of alliance and an over-arching structure creates hindrances in civil-military cooperation. The lack of official military participation in cyberspace has created a knowledge and information sharing gap between organizations. Lack of cybersecurity laws, as per international standards, creates a grey area for human rights. Lack of civil-military cooperation in cybersecurity sends a message to the world that civil-military organizations are not on the same page. Lack of policy hinders Pakistan chances of defending its cyberspace and recruiting more cyber experts to deal with cyber incidents.

It may be suggested to incorporate civil information sector experts within the military. It may also be suggested for incorporation of free communication and facilitation of information across civil-military sectors. The civil sector may assume greater responsibility to formulate and establish an overarching authority for better chances of civil-military cooperation. It is also suggested Civil sector acquire military expertise for securing civil cyberspace. Civil-military organizations could enhance CIMIC through jointly building indigenous technologies, reduce trust deficit for better capacity building. Indigenization of technology will help in securing cyber gateways and regulating information without infringing human rights.

Civil and military organizations must realize the importance of civil-military cooperation in cyberspace. The open communication lines could provide for more

avenues of cooperation: a platform to resolve the differences and formulate a roadmap for robust cybersecurity. This will help send a positive message of both sectors working together and securing the country's cyberspace from malicious cyber threats. The cooperation will help in creating a knowledge economy and in boosting the countries e-commerce. Cooperation is needed to help in cyber preparedness for any unknown cyber threat.

References

Ali, Y. F. (2015, June 05). Pakistan's National Security Council. *Pakistan Today.* https://www.pakistantoday.com.pk/2015/08/10/pakistans-national-security-council/

Aziz, F. (2018). Pakistan's CyberCrime Law: boon or bane? Heinrich Boll Stifung. https://www.boell.de/en/2018/02/07/pakistans-cybercrime-law-boon-or-bane

Baloch, S. (2016, December 31). Cyber Security is a matter of National Security. *Dawn.* https://www.dawn.com/news/1229738/cyber

Bolobhi. (2015). The Cybercrime bill and call-to-action. BoloBhi. https://www.dawn.com/news/1229738/cyber

Braun, M. A. (2005). Civil-Military Cooperation as vital part in the stabilization-process in Afghanistan. MA Dissertation, University of Postdam.1-27. https://www.grin.com/document/116894

Bischoff, P. (2020). Which countries have the worst (and best) cybersecurity? Comperitect. https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/

Church, R. L., Scapparra, M. P., & Middleton R. S. (2003). Identifying the Critical Infrastructure: The Median and Covering Facility Interdiction Problems. *Annals of Association of American Geographers, 94*(3), 491-502. https://www.tandfonline.com/doi/abs/10.1111/j.1467-8306.2004.00410.x

National Center for Cyber Crime. (2016). Prevention of National Cybercrime Act 2016. Pakistan National Response Center for CyberCrime (NR3C). http://www.nr3c.gov.pk/cas.html

Firdous, A. (2018). Cyber Security Issues in Pakistan. *Center for International Strategic Studies* https://ciss.org.pk/cyber-security-issues-in-pakistan/

Fravel, M. T. (2015). China's New Military Strategy: "Winning Informationized Local Wars." *Jamestown Foundation: Global Research and Analysis.* https://jamestown.org/program/chinas-new-military-strategy-winning-informationized-local-wars/

General Data Protection Rule. (2016). Article 7. Conditions for Consent. https://gdpr-info.eu/art-7-gdpr/

What is Cybersecurity? (2020). June 15, 2020 https://www.itgovernance.co.uk/what-is-cybersecurity

Greenwald, G., & MacAskill, E. (2013, June 11). Boundless Informant: the NSA's secret tool to track global surveillance data. *The Guardian.* https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining

Grigovrov, G. (2017). Emergence and development of civil-military cooperation. *De Gruyer Open: International Conference Knowledge-based Organisation*, XXIII(1), 119-123. = https://content.sciendo.com/view/journals/kbo/23/1/article-p119.xml?language=en#:~:text=Civil%2Dmilitary%20cooperation%20is%20a,which%20military%20operations%20are%20conducted.

Hassan, R. T. (2019, May 16). Cyber Security threats: policy gaps, challenges and way forward. *Daily Times.* https://dailytimes.com.pk/352011/cybersecurity-threats-policy-gaps-challenges-and-way-forward/

Heinl, C. H. (2015). Enabling Better Multinational and International Military Cooperation for Cyber-Related matters across Asia and Europe. *Center of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological Studies (NTU).* https://www.files.ethz.ch/isn/189457/PR150307_Military-Cooperation.pdf

Huntington, S. P. (1957). The Soldier and the state: the theory of politics of Civil-Military relations. Cambridge: Belknape Press of Harvard University Press. https://books.google.com.pk/books?id=1PqFe0rsfdcC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Hussain, F., & Bukhari, G., (2014). Communication surveillance in Digital Age. *Global Information Social Watch.*

https://www.giswatch.org/en/country-report/communications-surveillance/pakistan

Ministry of Electronics and Information Technology. (2013). *National Cyber Security Policy, 2013*. Indian Ministry of Electronics and Information Technology. https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/India_2013_National_cyber_security_policy-2013(1).pdf

Privacy International. (2015). Tipping the scales: Security and Surveillance in Pakistan. Privacy International. https://privacyinternational.org/sites/default/files/2018-02/PAKISTAN%20REPORT%20HIGH%20RES%2020150721_0.pdf

Jabri, P. (2018, February 18). Pakistan to develop e-governance council for policy formulation. *Business Recorder*. http://www.brecorder.com/2018/02/13/398914/pakistan-to-develop-e-governance-council-for-policy-formulation/

Janjua, R. W. (2010). Civil Military Relations: the impact of internal and external factors shaping the balance in civil military relations. Islamabad: *NDU Journal*.

Kemp, S. (2020, February 18). *Digital 2020:* Pakistan [PowerPoint Slides]. Datareportal. https://datareportal.com/reports/digital-2020-pakistan

Khalil, B. (2020, February 14). Emerging Warfare threats to Pakistan. Modern Diplomacy. https://moderndiplomacy.eu/2020/02/14/emerging-cyber-warfare-threats-to-pakistan/

Boeke, S., Veenendaal, M., & Heinl, C. (2015). Civil Military Relations and International military Cooperation in CyberSecurity: Common Challenges and State Practices Across Asia and Europe. In M.Maybaum, A.M. Osula, L.Lindstorm (Eds.), *7th International Conference on Cyber Conflict*: *architecture in cyberspace. Tallinn* (pp.69-80).NATO CCD COE Publication. https://www.ccdcoe.org/uploads/2018/10/CyCon_2015_book.pdf

NATO STANDARD AJP-3.19 Allied Joint Operation for Civil Military Cooperation Addition A Version *1* (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757080/20181112-dcdc_doctrine_nato_cimic_ajp_3_19.pdf

NATO/OTAN. (2020). Cyber defense. NATO/OTAN. https://www.nato.int/cps/en/natohq/publications.htm

NATO/ OTAN (2020). Relations with Pakistan. NATO/ OTAN. https://www.nato.int/cps/en/natohq/topics_50071.htm

NATO/OTAN (2020). A Comprehensive approach to Crisis. NATO/OTAN.https://www.nato.int/cps/en/natolive/topics_51633.htm

NATO/OTAN (2020). Science for Peace. *NATO/ OTAN*.

National Internal Security Policy 2014-2018 (2014). Pakistan Ministry of Interior.: https://nacta.gov.pk/wp-content/uploads/2017/08/National-Internal-Security-Policy-2014.pdf

Pernik, P., & Emmet, T. (2014). Interagency Cooperation on Cyber security: The Estonian Model. *International Center for Defense Studies*.

Qadeer, M. A. (2020, June 06). The Cyber Threat facing Pakistan. *The Diplomat*. https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/

Rafiq, A. (2019). Challenges of Securitizing Cyberspace in Pakistan. *Institute of Strategic Studies Islamabad*. 6(1), 90-101. http://issi.org.pk/challenges-of-securitising-cyberspace-in-pakistan/

Rajoka, K. U. (2020, June 16). Where does Pakistan stand? *Business Recorder*.https://www.brecorder.com/news/1004662/where-does-pakistan-stand

Raska, M., & Ang, B. (2018). Cyber Security in South Asia. DGRIS, Asia Center. https://centreasia.eu/wp-content/uploads/2018/12/NotePre%CC%81sentation-AngRaska-Cybersecurity_180518.pdf

Salmaan, L. (2018). Integrating Cyber Security and Critical infrastructure: National, Regional and International approaches. *Stockholm International Peace Research Institute*. https://www.sipri.org/sites/default/files/2018-04/integrating_cybersecurity.pdf

Sarbannes-Oxley Act of 2002 (2010). https://pcaobus.org/About/History/Documents/PDFs/Sarbanes_Oxley_Act_of_2002.pdf

Syed, R., Khaver, A. A., & Yasin, M. (2019). Cyber Security: Where does Pakistan Stand? *SDPI Working Paper, 167*. https://think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1

National Center for Cyber Security (2020). *Research Areas*. May 29, 2020 http://www.nccs.pk/collaborations/research-area

Pakistan is facing issue of cyberattack (2015). CustomToday. https://customstoday.com.pk/pakistan-is-facing-issue-of-cyber-attack/?__cf_chl_jschl_tk__=75446c822acb4668d36c4cc9431b9764ba40d6e2-1593003456-0AQdrSVdWfqGWM6sEEk40EqK1A_a420vDLBk0WCIf79jUPV5Aa1eJJCpICjZtulscu56cVcEvMd_a7PZn_U4thB9eAurc1EKmrQbm7QORSWTkL4rErEt7Szetoe1pAzsVgNh2YMyFaC3I74SE2FcbEqOe2iQfNUdupGDWpFk6CS-bjStpErRkbDTOH96eD1OJFhWTBEiSqbsShf5jpg1imdk83_HJIGoP3d0H0TeYw8-JBv-S_kKqhrP8ubrF1cO7FPY2Yj51lumE5iTmgI48kqk53sMUmZ7dTdIKgXATBuS0qmRi0eL0Toe28k1_vPRvSlfxobdRPQpxipC8OAXQCVA

International Telecommunication Union (2018). *Global Cybersecurity Index 2018*. ITU Publication https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

International Telecommunication Union (2020). *Definition of Cybersecurity*. ITU. https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

UN Open ended Working Group (2019). Bridging the Cyber Norms debate with evidence. Cape Town: Research ICT Africa. https://www.un.org/disarmament/wp-content/uploads/2019/12/Discussion-Paper-OEWG-Intersessional-Meeting.pdf

Vombetkere, S. G. (2018, April 06). Cyber Security: Civil and Military Implications. Indian Defence 33.http://www.indiandefencereview.com/news/cyber-security-civil-and-military-implications/

Work, J. D. Janensen, B. (2018, September 04). *Cyber Civil-Military Relations: Balancing interests on the digital fronties*. War on Rocks. https://warontherocks.com/2018/09/cyber-civil-military-relations-balancing-interests-on-the-digital-frontier/

Yamin, T. (2014). Information CBMs between Pakistan and India in Cyberspace. Islamabad: NUST Publishing.

Yamin, T. (2018). Cyberspace Management in Pakistan. *Governance and Management Review (GMR)3(1),46-61*. http://pu.edu.pk/images/journal/IAS/PDF/4-v3_1_18.pdf