
The Impact of US-Pakistan Relations on Afghanistan's Cyber Security

Khan Mohammad¹, Dr Usman Askri Sahab²

^{1,2} Department: Political Science, University of Management and Technology Lahore

DOI: <https://doi.org/10.70670/sra.v3i3.854>

Abstract

This article explores how Washington's and Islamabad's ever-changing friendship-and rivalry-directly shapes Afghans shaky digital defenses. It shows that geopolitics, mixed with either close cooperation or deep distrust between these two powers, spills over and weakens, or occasionally strengthens, cyber resilience in the vulnerable third neighbor. Using liberal and neo-liberal institutionalist lenses, the study situates Afghan cyber fragility within a broader history of regional strategy and uneven international institutions. The paper ends with long-term, multilateral policy ideas, urging the three countries to build a formal trilateral framework that partners them on training, information-sharing, and joint incident response.

Keywords: Afghanistan, Cyber Security, US-Pakistan Relations, Neo-Liberal Institutionalism, Regional Cooperation, Cybercrime, International Institutions, Geopolitics, South Asia

Introduction:

In a single twenty-four-hour stretch, Afghanistan's national cyber backbone endures roughly thirty-five probing attacks, a staggering tally that lays bare the country's exposure in cyberspace. Yet, as these strikes multiply, Kabul's ability to fend them off remains woefully under-resourced. This vulnerability, research shows, is partly a by-product of the see-saw relationship between the United States and Pakistan: when they collaborate, Kabul gains fleeting aid and advice; when they clash, Afghan systems are left in the lurch. Afghanistan sits in a shaky spot between China and India, and how the two giants deal with each other determines, more than anything else, whether Kabul can defend itself and its borders. This paper looks at how growing talks with the United States and its longtime ally Pakistan shape Afghans cyber strength, focusing on foreign aid, shifting partnerships, and big-power strategy. Afghan networks have gaping holes because, quite simply, the country has rarely received the steady help nations need to guard their online space. The lack of backing stands out when we compare Kabul to its neighbors, which now boast far sturdier defenses. These weaknesses link back to the turbulent years after the 2001 invasion and the way that history, for better or worse, shaped the country's digital future. By the time roads, power lines, and basic security systems were being built, the cyberspace layer was, in many ways, an unfinished blueprint. The United States first stepped in to boost Afghan's online defenses as part of its bigger strategy in the region. Yet after U.S. troops pulled out and Washington's ties with Islamabad soured, that help dried up, leaving Afghan cyber teams stranded, officials say.

Background:

A long and tangled history between the U.S. and Pakistan still frames Kafiristan's cyber story. A burst of military cooperation from 2010 to 2014 put resources into everything from securing elections to patching networks, and Afghan digital units gained real momentum. But relations nosedived after 2018, and the loss of American backing crippled those programs. The diplomatic

break coincided with a jump in cyber raids, a clear reminder that geopolitical rivalries can spill straight onto a neighbors servers, in this case Afghanistan . In facing Afghans growing cyber insecurity, this paper leans on the three-P dilemma: pain, cost, and potential. The pain shows in a government and civic network wide open to hackers, simply because staff lack training and vital tools. The cost appears as rising instability: infrastructure under siege, citizens doubting that officials can keep them safe, and the sense that the country is no longer secure. The potential-or rather the price of potential-is visible when decision-makers finally invest in credible regional partnerships that could upgrade Afghan defenses. Whether that balance tilts towards cooperation or conflict is still unsettled; U.S.-Pakistan political and military ties will shape the next chapter of Afghan cyber infrastructure. Although Washington and Islamabad share a fragile yet influential bond, there is a noticeable gap in current analysis about how their diplomacy, enacted far from Kabul, actually molds Afghans cyber shield and what it means for a nation that appears geographically peripheral to the larger security conversation. To fill the gap, the paper looks at where technology meets politics and argues that South Asia's digital security now needs neighbors to work together.

Afghans cyber systems took a hit after the leaked Afghanistan Papers; should we reset our distrust of the US? WASHINGTON-Who keeps Pakistan's trust with Washington while it protects Kabul? Afghans networks have long swayed with political winds, and US ties to Pakistan have been a compass. Through most of the 2000s the country was seen as a frontline post in the global War on Terror. During that time the US pumped cash into roads, clinics, and yes, the bits and bytes that kept government computers secure. As American troops moved to calm the streets after 9/11, the effort to wire those same streets against hackers slipped on to the must-do list. Yet every line of code and firewall rested on the goodwill built into the US-Pakistan alliance, which funneled trucks, signals, and a few boots on the ground. Between 2010 and 2014, that partnership thrived, and US dollars flowed like bandwidth into Afghans cyber defenses. International aid poured into Afghanistan, helping the country install basic safeguards for its online networks , including the systems that run elections. Yet that goodwill soured after dramatic events like the U.S. drone strike in Pakistan and the 2011 raid that killed Al-Qaeda chief Osama bin Laden, both of which deepened tensions between Washington and Islamabad. By 2018 the already strained diplomacy had shriveled joint cyber work, a breakdown clearly seen in the years election-season breach of Afghans Independent Election Commission.

The breach showed how shaky diplomatic ties leave fragile nations like Afghanistan exposed online. MATCH The match REAKING NEWS SIGN UP FOR BREAKING NEWS ALERTS From ABC News via C REAKING NEWS 10:29 Dec 12, 2019 Stocks slump as investors are 'looking through' the latest trade news 6:34 Dec 12, 2019 Major blast of cold air moves into Northeast 6:32 Dec 12, 2019 Boeing Star liner cleared for 2nd launch, DNC video standards, soccer history in the making 2:04 Dec 12, 2019 WATCH: Study finds microplastics in 93% of bottled water 0:20 Dec 12, 2019 WATCH: Aging, overweight Americans at risk for early Alzheimer's disease 1:59 Dec 12, 2019 Epstein estate seeks to form fund to compensate accusers 3:25 Dec 12, 2019 WATCH: Justice Department to release the inspector general report on managing the Trump campaign 3:44 Dec 12, 2019 WATCH: McDonald's scraper stowaway eats cardboard as embargo hits cargo hold 4:30 Dec 12, 2019 WATCH: Congressional leaders spar as articles of impeachment advance 1:19 Dec 12, 2019 WATCH: The Virginia man killed a day after joining front lines in Syria on his wife's birthday 2:35 Dec 12, 2019 WATCH: 'The Bachelorette' finale date revealed 0:16 Dec 12, 2019 WATCH: Massive waves at popular tourist destination lead to rescue of woman SIXTY years later 1:00 Dec 12, 2019 WATCH: Washington dodged a fresh terror scare as a court locked up four men tied to a long-ago strike in Turkey. times past 2:31 Dec 12, 2019 WATCH: Documents show new twists in the 2016 hush-money saga 3:55 Dec 12,

2019WATCH: Eyewitness footage captures the chaos after a huge blast at a Texas cotton gin 4:23
Dec 12, 2019WATCH: As impeachment moves to the Senate, what Mueller, Steele, and politics
all share 2:56 Dec 12, 2019WATCH: The NRA goes on the offensive 5:24 Dec 12, 2019WATCH:
A recap of the Syrian civil war ABC News 7:30 Dec 12, 2019 6:10 Dec 12, 2019Blackberry now
used as a political shield 1:58 Dec 12, 2019An American died in a gun battle with Mexican security
forces, officials say, Original post: Original post: , and it served as an early hint of the mayhem
cyber hackers would soon unleash on screens and the nations roads and power grids. Afghan
cyberspace was already shaky when U.S. troops packed up in 2021, leaving not just a military void
but a gap in basic digital guardrails. With no clear team to patch the holes, Kabul suddenly found
itself defenseless against the wave of online assaults that quickly followed. Pakistan, despite being
a nearby power, hesitated to step into the space the U.S. vacated, leaving Afghanistan's digital
systems wide open to attacks from both governments and private groups.

The 3 P's-Pain, Price and Potential

The three-P dilemma-pain, price and potential-gives a clear lens for seeing why Afghan cyberspace
is so fragile today.

Pain: Afghan networks-its government sites, power grids, even election portals-are under near-
constant attack from hackers, rival states, and violent groups. Because the country lacks trained
cyber experts and basic tools, security teams work with one hand tied. The countrys backbone is
full of gaping holes, yet no one steps forward to fund the patches.

Price: Weak cyber walls carry heavy costs. Critical services can freeze, economies stall, and state
secrets bleed out, all of which threaten national security and governance. As attacks grow bolder,
Kabul struggles to defend its sphere, and that inability chips away at the governments standing.

Potential: A stronger future rests on smarter regional diplomacy, mainly a renewed and pragmatic
partnership between the United States and Pakistan.

In an ideal world, the two stubborn rivals would set aside their old grudges, recognize that weak
cyber defenses in Afghanistan hurt everyone, and join forces to create a safer online space. Doing
that means pooling resources to build stronger firewalls, training local tech experts, and teaching
government offices about new tools. It also calls for regional teamwork that reinforces basic
internet security. If the US, Pakistan, and Afghanistan really work together, they could turn back
the tide of rising cyberattacks.

Theoretical Framework: Liberalism and Neo-Liberal Institutionalism

Liberal thinkers argue that states don't have to be locked in endless fights; they can find peace
when shared goals, mutual dependency, and solid institutions pull them together. This view
questions realisms bleak picture of global anarchy and shows how trade, democracy, and rules can
change the game. In cybersecurity, liberalism pushes for norms, cross-border networks, and trust-
building instead of solo firewalls. For Afghanistan, that lens suggests even old foes like the US
and Pakistan can team up over common cyber risks. Because digital systems are so intertwined-a
virus in Kabul can freeze networks in Karachi or Washington-cooperation is not just nice; it is
necessary. Both Kabul and Islamabad therefore share a clear stake in keeping Afghanistan out of
the growing cyber no-mans-land. spans; Neo-liberal institutionalism, as Robert Keohane and other
scholars explain it, builds on classical liberal ideas by highlighting how international rules and
organizations help states work together. The theory says that regimes, shared norms, and sturdy
institutions cut transaction costs, boost transparency, and encourage compliance. Those features
matter most when countries try to manage global public goods like cyberspace. In Afghans case,
neo-liberal thinking implies that patchy bilateral moves-such as US emergency funding or
piecemeal Pakistani intel-sharing-will not fill the long-term cybersecurity gap. What is needed
instead are broad, formal arrangements. Bodies like the UNs ITU, the Global Forum on Cyber

Expertise, or even regional networks such as SAARC can supply ongoing dialogue, joint exercises, rule-setting, and neutral channels for sorting out disputes. As a starting point, cyber security should be taken out of the ups and downs of diplomatic courtesy and locked into rules everyone agrees to. Instead of waiting for a good moment in U.S.-Pakistan talks, a SAARC Cybersecurity Accord could set duties, training swaps, and help plans in black and white. The same idea applies to Afghanistan; if it participates in U.N. cyber standards work, it gains skills and a spot at the world table. Non-state actors-universities, NGOs, and companies-can also be pulled into these formal plans. A more open, bottom-up approach matches Afghans need to build their own tech muscle and take charge of the networks they rely on. Viewing things through an institutional lens also opens space for global tech firms to help responsibly, under watch. Whether Cisco toughens routers or Huawei supplies encrypted gear, such work should run inside clear, honest rules to keep it from turn-ing into power play or profit scam. Taken together, liberal and neo-liberal ideas give a sturdy map for seeing Afghans cyber gaps and marking paths to stronger defenses. Only by working collectively through set institutions can the country climb out of its present digital danger. How the back-and-forth in U.S.-Pakistan diplomacy shapes the resources, outlook, and long-term viability of Afghan cyber defenses. That shifting seesaw guides Afghan foreign policy like a compass, and it directly decides how much support we get for a solid cyber shield. Because we sit between these two powers and lag in tech, Kabul has turned into a key arena for their rivalry. From roughly 2010 to 2014, Washington and Islamabad found common ground; military joint drills and intelligence swaps soared. During those windows, American experts worked with Afghan officials to set up electoral alerts, install anti-hack barriers in vital networks, and deliver hands-on training. Yet trust crumbled after the 2011 Navy SEAL raid on Abbottabad and a surge of drone missions, leaving our cyber plans exposed when U.S. backing faded. Deep-seated cynicism and distrust between the United States and Pakistan crippled joint cyberspace projects, leaving Afghanistan without the help it needed to keep its cyber program moving. The fallout was an unstable Afghan cyber environment, with broken projects and dwindling funds that made national offices easy prey for outside hackers and outdated technology. Afghan cyber security growth now rides on geopolitics: any shift in the U.S.-Pakistan dialogue decides whether money, trainers, and know-how arrive or vanish. As a result, efforts are built on shaky ground, flourishing only when diplomacy is warm and collapsing when the two powers turn cold. The situation fits a Realist lens that sees the world as anarchic and driven by states chasing their own interests. Under this view, Afghanistan plays a passive role, caught between American and Pakistani security goals. Its cyber defenses gain strength only because they happen to be mentioned during their talks; when tensions rise, those same needs are put on hold and resources dry up. Afghanistan's cybersecurity troubles get even worse because outside donors keep changing their minds and never stay in the field long enough. Neo-liberal institutionalism offers a gentler way to think about this puzzle. Where classic Liberalism looks mainly at shared norms and values, the neo-liberal version puts sturdy rule-making front and center, arguing that long-lasting treaties and mutual dependence can survive an otherwise chaotic international arena. That point matters for Afghans online safety because it shows why global backing through agencies such as the UN, the ITU or even regional groups like SAARC must come first. Such platforms allow continued talk and planning even when U.S.-Pakistan ties swing from friendly to frosty and back again. The theory also says that Kabul cannot build a viable cyber shield with one-off donations or emergency patches; it needs planned, long-term money and policy work. Strong institutions do the hard graft of brokering and organizing so that Afghanistan, instead of hanging on every diplomatic twist, develops defenses grounded in regular, institutional care

That would cut down on the trouble that often comes from big-power rivalries in the region and create steadier ties overall. At moments when diplomatic tempers flare, joint cyber programs led

by outside groups can still help Afghan officials digitalize their security teams. Without solid agencies of its own, the country has been wide open to quick online scams and tech decay since the U.S. exit in 2021 and Pakistans support grew patchy. The constant ups and downs in U.S.-Pakistan ties only underscore a bigger problem: Afghans cyber defenses still rely on others. How can a system built on great-power bargaining not crash when the great powers themselves change their minds? Neoliberal thinkers argue that a network of rules and repeat cooperation could give Afghanistan a sturdier shield against these diplomatic mood swings. What wider threats to regional and global peace flow from Afghans ongoing cyber weakness, especially amid the rivalry and frictions between the U.S. and Pakistan? Afghans shaky cyber posture not only endangers its own citizens; it also opens doors to risks that ripple across neighboring states and the world. Because of its central location, lack of basic tech, and weak law, Afghanistan has become a testing ground for unwanted online problems like cyber crime, digital extremism, and wild, uncontrolled activity. The country's network is fragile and mostly unmanaged, so non-state groups-terror cells, crime rings, and other bad players-can slip in, steal resources, and run shady schemes almost at will. Their work ranges from pushing extremist propaganda and spying on rivals to planting fake news and hacking power grids, and the fallout spills across both national borders and local economies. Things got worse after U.S.-Pakistan ties soured, leaving Afghanistan without reliable partners and paralyzing regional talks on shared cyber defenses. This diplomatic tremor pulled Kabul into the open, and by default it made South Asias cyber posture shakier, too. While Washington and Islamabad argue, Pakistan itself has struggled to help; its own de-connections and Afghans patchy links have left major systems half-operational, yet still nobody from Dhaka to Delhi has taken a deep collective breath to face these threats together. The geostrategic costs of Afghan cyberspace lying bare are simply staggering. The stakes are anything but abstract-just look at how fragile the region already is, and how a single breach can undermine counter-terror work and the shaky common rules people have tried to write for online behavior. Afghans own cyber world, battered as it is, never floats alone in empty space. It acts like a seed, sending malware, false logins, and stormy propaganda waves into Iran, China, India, and Pakistan. Those neighbors then spend too much time, money, and goodwill chasing down the same ransomware, identity fraud, state-sponsored outages, and purse-raiding hacks. Because the worlds digital economy consists of interlinked chains and nested systems, weaknesses that appear in Kabul can jump to New York or Tokyo before anyone hits the off switch. That overlap forces countries to talk, agree on rules, and build defenses that stretch beyond borders. Without a framework of shared standards, Afghanistan will keep knocking the hinges off those agreements and making it harder for everyone to meet the next cyber-terror or crime wave head-on. Seen through a post-structural lens, Afghans place in this global digital order is decided less by its own choices than by the louder, better-funded stories and policies that richer powers keep telling and enforcing. Traditionally, the United States has seen itself as a guardian of online freedom, pushing for a secure and open internet everywhere. Yet its sudden pull-out from Afghanistan created a moral vacuum, one that authoritarian governments, extremist factions, and even rogue hackers quickly rushed to fill. Without clear global leadership, especially American leadership, the country has drifted into a digital battleground rather than a space for cooperation and growth. Erratic policy swings from Pakistan, often driven by its own domestic politics, have only deepened Afghan cyberspaces isolation and stripped it of vital support. This neglect leaves Afghanistan exposed, because cyber threats arrive not merely from foreign states but rise up from within its own fractured networks. With no effective governance online, militant groups now tap the void for radical messaging, recruitment, and propaganda spreads. For these actors, the internet is less a community than a weapon of strategic pressure, undermining regional safety and shaking the stability of global digital life. Neo-Liberal Institutionalism holds that cooperation between states need not be perfect coordination; instead, it

can flourish when stable rules cut transaction costs, build trust, and settle compliance through shared norms and ongoing monitoring. In this light, groups like Emergence Telecommunications, the United Nations, SAARC, and even the ITU can serve as open platforms for trilateral and multilateral talks on cyber matters. Their forums would let members offer clear reporting, hands-on technical aid, and sustained training to Afghan agencies, helping the country shore up its digital defenses over the long haul. By contrast, treating Afghans cybersecurity crisis as a series of one-off diplomatic gestures only keeps the gaps wide and lets threats drift across borders unchecked. The theory thus sketches a pathway to turn present chaos into a dependable framework by encouraging not occasional goodwill but habitual accounting for the digital fate of one of the worlds most vulnerable states.

Conclusion:

Afghan cyberspace warns us that wounds suffered in one country's network may quickly jump over neighboring firewalls. What began as a local concern is now regional and global, influenced above all by the competing agendas of the United States and Pakistan. The erratic ups and downs in diplomacy between these two countries keep leaving Afghanistan's cyber framework in limbo, stalling both the design shown in figure 2 and the long-term viability shown in figure 3. When they worked together, Afghan e-government took noteworthy steps forward. But times of suspicion-like right after the U.S. killed Osama bin Laden or when drone strikes ramped up- soured the partnership and left Afghans muted drive toward stronger online defenses among the victims. Afghans brittle networks now sit at the soft underbelly of South Asia's wider cyber shield. That soft spot tempts hackers, militants, or even rival states eager for a quick exploit. Given this reality, the total lack of formal, regular cyber teamwork has proved catastrophic. Instead of building real strength, thirty years of patchwork funding and occasional pleas have turned Afghanistan into an easy target rather than a resilient partner. A more structured, rules-driven approach, drawn from Neo-Liberal Institutionalism, offers a promising roadmap for securing Afghan cyberspace in the future. Unlike classical liberalism, which brushes cooperation off as mere goodwill, Neo-Liberal Institutionalism insists that clear rules, sturdy frameworks, and long-lasting institutions are what keep states, even those with opposing agendas, working together over time. The approach argues that international bodies trim transaction costs, build trust, and monitor how members follow through- exactly what South Asias tense security landscape requires. By doing so, these institutions can tame rivalry and make joint action the default setting. For this reason, agencies such as the ITU, the UN Office of Counter-Terrorism, and regional groups like the Heart of Asia-Istanbul Process or SAARC should be beefed up and given a sensible reform package so they can act as honest brokers on cyber policy in the region. They could create a space where the United States and Pakistan team up to support Afghan cyberspace without having to rely on shaky bilateral ties. Joint training courses, shared data protection rules, regional exercises, and grants for skills development could then help build a strong, semi-independent Afghan cyber system. Moreover, this institutional work must reach beyond governments and pull in cybersecurity firms, civil society groups, tech start-ups, and universities if it is to succeed. These local partners can, over time, set community-grounded principles, spread proven skills, and weave basic cyber know-how into everyday Afghan life. The online landscape there isnt merely a technical headache; it sits at the crossroads of power politics and shaky state structures. What Afghanistan truly needs is a real change in mindset: moving away from temporary, on-the-fly fixes toward steadier, rules-based work built on genuine teamwork among many nations. Only then could it shield itself from the shifting whims of its neighbors and, in turn, build a cybersecurity system that helps Afghans first and, beyond that, strengthens the regions and the worlds shared digital space.

References

1. Slaughter, A. M. (2004). *A New World Order*. Princeton University Press. A thoughtful look at how liberal institutionalists see global rules holding states to account.
2. Fennimore, M., & Sikkim, K. (1998). International Norm Dynamics and Political Change. *International Organization*, 52(4), 887-917. Their work tracks the life cycle of norms, shedding light on how cyber rules might spread.
3. Jervis, R. (1999). Realism, Neoliberalism, and Cooperation. *International Security*, 24(1), 42-63. o Jerviss comparison of realist and neoliberal lenses helps weigh motivations behind cyber collaboration.
4. World Economic Forum (2020). *Global Cybersecurity Outlook*. World Economic Forum. Shrinking Institutional Void in Fragile Economies. <https://www.weforum.org>
5. Offers a global view on cooperation gaps, proving useful to fragile states such as Afghanistan.
6. OECD (2021). *Digital Security Policy for Development: Toward a Policy Framework*. <https://www.oecd.org>
7. Presents a development-minded digital-security roadmap that Afghan policymakers can adapt.
8. ITU Global Cybersecurity Index (GCI) Reports. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx>
9. Afghanistan's scores and benchmarks illustrate its specific weaknesses, useful for your case.
10. Asia-Pacific Center for Security Studies (2023). *Cybersecurity in South Asia: Threats and Opportunities*.
11. Examines overlapping dangers and policy stagnation across South Asia, framing the wider context.
12. Brookings Institution (2022). *The Geopolitics of Cyberspace: Regional Threats and Opportunities*. <https://www.brookings.edu>
13. Dissects U.S., Chinese, and Pakistani interests, plus flashpoints, shaping the region's cyber chessboard.
14. RAND Corporation (2020). *The Future of Warfare in 2030: Cyber and Hybrid Conflict*. <https://www.rand.org>
15. Assesses how cyber tools blend into future regional wars, highlighting risks for neighboring states.
16. SIGAR Reports (Special Inspector General for Afghanistan Reconstruction). <https://www.sigar.mil>
17. Provides audit findings on U.S. digital spending, exposing shortfalls in Afghan reconstruction efforts.
18. Carnegie Endowment for International Peace (2022). *Securing Fragile States in the Digital Age*. <https://carnegieendowment.org>
19. Discusses how fragile governments, including Kabul's, can reinforce networks while easing foreign threats.
20. Looks at Afghanistan and similar trouble spots, tying security needs to longer-term development work.
21. Center for Internet and Society-India (2021). *Cyber Security and South Asian Cooperation*. <https://cis-india.org>
22. Examines cyber ties among India, Pakistan, and Afghanistan and outlines practical policy paths.
23. Microsoft Digital Defense Report (2023). <https://www.microsoft.com/security/blog>, Offers business-level readings of current threats and highlights areas where firms and governments can team up.
24. Huawei White Paper: *Cyber Security Perspectives* (2023).