

Protocol Manipulation and Strategic Aggression: A Technical Review of Cyber Warfare in Modern Geopolitical Conflicts

Pranjal Tripathi¹, Aarti Goswami²

¹Devi Ahilya Vishwavidyalaya School of computer science and IT

²Mata Gujri mahila Mahavidyalaya jabalpur Department of computer science

Corresponding Author

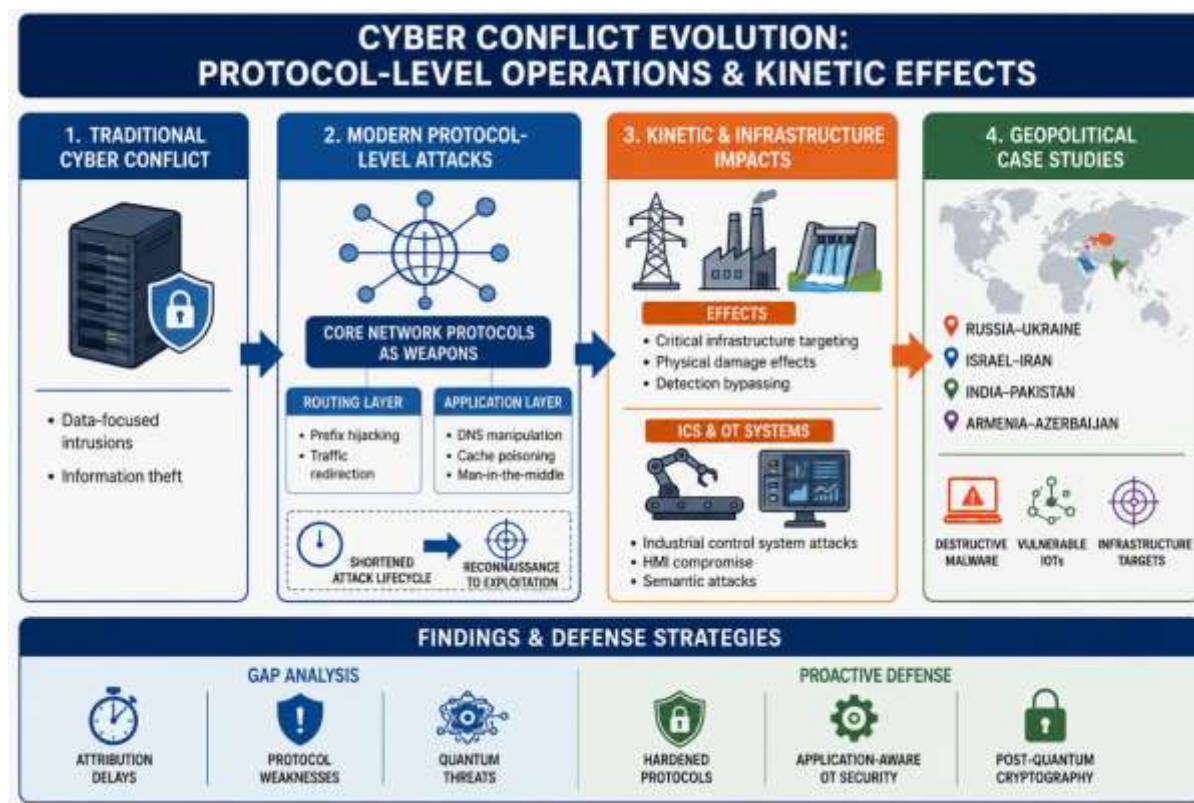
Pranjal Tripathi

pranjaltripathi7781@gmail.com

Devi Ahilya Vishwavidyalaya

School of computer science and IT

Graphical Abstract:



Highlights

- Cyber conflict is shifting toward protocol-level attacks targeting critical infrastructure with national-scale impact.
- BGP and DNS exploitation enables traffic redirection, surveillance, and large-scale disruption.
- Cyber operations show a compressed lifecycle, reducing detection and response time.
- SCADA and OT systems are primary targets, enabling physical disruption through cyber means.
- The study highlights need for hardened protocols, OT security, and post-quantum cryptography for resilience.

ABSTRACT

Modern cyber conflict has transitioned from data-focused intrusions to protocol-level operations that have the potential for kinetic and national scale disruptive effects. This work provides a technical characterization of the concrete ways in which state and non-state actors have been using fundamental networking protocols across routing, application, and industrial control layers as weapons. Cyber operations have come to share a shortened lifecycle in which reconnaissance appears almost indistinguishable from exploitation, allowing for near-instantaneous compromise of critical information infrastructure (CII) with unprecedented timing and impact. This paper studies the use of core internet protocols such as Border Gateway Protocol (BGP) and Domain Name System (DNS) for exploitation. Such techniques give adversaries capabilities to redirect traffic, perform man-in-the-middle attacks, surveil data, and segment resource access (prefix hijacking, cache poisoning & resolution manipulation). The research also examines the weaponisation of Supervisory Control and Data Acquisition (SCADA) and Operational Technology (OT) environments, highlighting advanced semantic attacks aimed at compromising human-machine interfaces that enable physically destructive effects without triggering any traditional detection methods. These methods are illustrated through geopolitical case studies Russia-Ukraine, Israel-Iran, India-Pakistan and Armenia-Azerbaijan—that show real world applications of these techniques (e.g. deployment of destructive malware, vulnerable IoTs used as proxy weapons or targets for cyber-attacks against critical infrastructure). According to the results, there is a consistent pattern of usage of legacy protocols, weak configurations, and incomplete security adoption. The identified important gaps are on attribution latencies, protocols-resilience & quantum threats to CR systems. It promotes proactive defence with hardened protocols, application-aware OT security and post-quantum cryptography adoption as a means to complement global cybersecurity resilience frameworks.

KEYWORDS: Cyber Warfare; Protocol Exploitation; Critical Information Infrastructure (CII) ; SCADA and Operational Technology Security ; Post-Quantum Cryptography

1. INTRODUCTION

Cyberspace has changed the face of warfare as an entirely new theater of conflict; warfare is no longer fought between armed personnel in battlefield encounters, or scripts inserted into mainstream networks the front line has been pushed back to deeply-embedded aspects of our interconnected network infrastructures.(1) Modern cyber warfare goes beyond data stealing or new-age espionage, and more towards a degree of inducing kinetic and large-scale disruption by actively misusing fundamental networking protocols. These operations specifically focus on the Critical Information Infrastructure (CII) components such as energy grids, communication systems, transportation networks, healthcare services and financial institutions because a localized disruption to a CII could easily escalate into societal, economic and national security attendant risks. The interconnectedness of these systems increases risk as failures in one area can quickly spread through many sectors.(2) Formal models that describe each phase of modern cyber operations typically classify these in terms of a structured lifecycle which includes phases such as reconnaissance, weaponisation, delivery, exploitation, installation and command-and-control (C2), followed by actions on objectives. But with the new breed of attacks like attack automation, AI-assisted reconnaissance and pre-positioned access the lifecycle got resurfaced as minimal.(3) This capability allows adversaries to go from initial compromise to operational impact in near real time and, as such, changes the readiness requirement for their attacks they are faster and scaled larger. This compression poses a direct challenge to the customary, reactive paradigms of cybersecurity, which often are incapable of responding in real-time or near-real time upon threat discovery.(4)

One of the key drivers for this transformation is the merging between Information Technology (IT) environment and Operational Technology (OT) environment. While this integration improves operational efficiency and data-driven decision-making, it also expands the attack surface by connecting previously isolated industrial systems to threats on the internet.(5) Adversaries capitalize on the fact that many common protocols, including but not limited to Border Gateway Protocol (BGP), Domain Name System (DNS) and Server Message Block (SMB), can be exploited through inherent design limitations, legacy dependencies and inconsistent security implementations.(6) At the same time, industrial control systems especially Supervisory Control and Data Acquisition (SCADA) architectures, which regulate physical processes directly have become major targets for exploitation popularity. Such attacks may mean not only the leak of data but also

very real physical damage, service interruptions, and endanger public safety.(7) In addition, the strategic goals of cyber operations have changed to include psychological impact, disruption of public trust and co-optation of state actors. This change reflects the wider militarization of cyberspace with not just state actors but also non-state actors deploying APT like techniques to obtain geopolitically secure objectives. These are the weaknesses of a protocol that can be exploited by attackers to operate under the radar, maintain persistence and deliver much more impact than resources invested.(8)

However, balancing the inertia of progress with security principles that have not been incorporated into foundational internet protocols and critical infrastructure systems is a monumental task.(9) Long-standing challenges, such as partial implementation of security frameworks (e.g., routing validation and secure name resolution), capability gaps in identifying stealth attacks to follow an end-to-end kill chain approach to detecting advanced persistent threats (APTs), and the difficulty of properly attributing cyber events prevent adequate defensive and policy responses.(10) Moreover, new technological advancements like quantum computing and artificial intelligence are introducing entirely new forms of threats, potentially increasing not just offensive power but systemic risk in different ways. In this context, the current review offers an in-depth and technology-centric overview of protocol-level Cyber warfare. It synthesizes existing knowledge about the abuse of core network protocols, studies geopolitical case studies to contextualize these threats in real-world terms, and pinpoints pressing research open problems relating to protocol robustness, attribution, and cryptographic strength. (11)The study also includes some recommendations with specific regard to strategic as well as policy strategies supportive of boosted cybersecurity resilience, through driven defense, framework protections alongside embracing evolving threat landscape adapted frameworks.

2. THEORETICAL FRAMEWORK OF PROTOCOL-LEVEL CYBER CONFLICT

2.1. Cyber Warfare Lifecycle

The cyber kill chain offers a general and widely-accepted model to analyze the pattern of today's information warfare. It defines a cyber-attack as a multi-step processes mostly consisting of Recon, Weaponisation, Delivery, Exploitation, Installation (of malware), Command-and-control (C2) and Actions on objectives. Phases This signifies a stage in the attack continuum where adversaries are able to effectively escalate from doing reconnaissance to actually performing mission specific goals. In the reconnaissance phase, attackers gather extensive information about their target systems, network topologies, and any usable weaknesses. By this intelligence it is then used in the weaponisation stage to craft specific evil payloads with the aim of exploiting a given vulnerability.(12) Phase 3: Delivery You send these payloads via vectors such as phishing emails, compromised websites or direct network intrusion. When these elements enter the target successfully, they exploit the victim and deliver programs that infiltrate and continue running in the environment. During the command-and-control phase, attackers communicate with and control compromised systems remotely; ultimately leading to actions on objectives such as data exfiltration, disruption of services, and infrastructure sabotage.(13) This lifecycle has been completely transformed in today's cyber warfare as it is compressed and automated. Now, advanced threat actors use AI in reconnaissance, exploit kits ready-made, and automated propagation methods to shrink the kill chain from an initial compromise to a business impact. This speed allows attacks to be carried out almost immediately which reduces the detection and response window. As a result, attack surfaces should rely more on proactive threat hunting and early stage detection mechanisms instead of being entirely reliant on reactive mitigation methods for defensive strategies.(14)

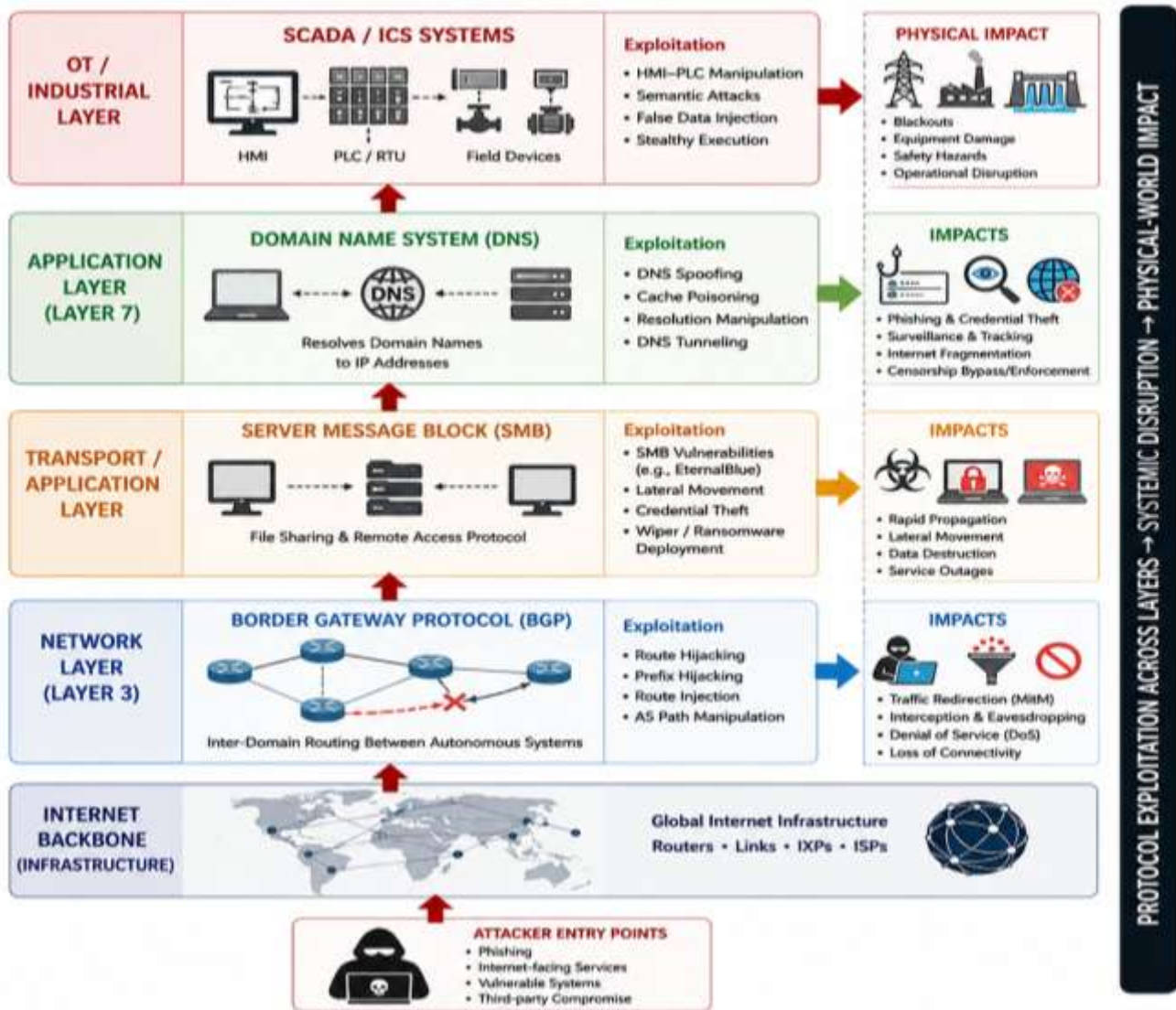


Fig 1. Protocol- level cyber warfare stack Model

2.2. Movement Towards Destructive Cyber Operations

In its early days, cyber operations were largely espionage-oriented: conducting surveillance and exfiltrating data for the purpose of strategic or economic intelligence. But the nature of the threat landscape has been on an obvious change to destructive and disruptive cyber operations. State-sponsored actors are now more in search of more than just access for information where their approaches include the disabling, denial, or total destruction of critical systems and services.(15) This change is largely tied to the increased convergence of IT (Information technology) and OT(Operational Technology) environments. The emergence of new attack vectors by converging industrial control systems with enterprise networks allowed adversaries to reach the bridge between digital systems and physical processes. Stated that dangerous cyber intrusions now manifest as direct and concrete threats, including outages of power supplies, damage to its industrial equipment and disruption of essential services for the public. (16)Furthermore, contemporary cyber operations are often focused on actually producing psychological and strategic impacts; e.g. the weakening of public trust or economic disruption alongside forcing action by state actors. The rise of destructive malware, wiper attacks and campaigns to cripple state infrastructure testify to this militarization of cyberspace in which combatants starting from against civilians. Such an evolution represents a paradigm shift in how cyber conflict is defined, with the exploitation of protocol-level vulnerabilities wielded as weapons with implications that extend beyond mere information dominance to include broader geopolitical and strategic ends.(17)

3. Exploitation of Core Internet Protocols

The global internet infrastructure is intrinsically reliant on a small suite of core protocols that manage routing, addressing and communication between distributed networks. These same protocols were originally devised for limited security but

have become prime targets for exploitation in modern cyber conflict. Adversaries exploit intrinsic design limitations, the absence of authentication mechanisms, and inconsistent deployment of security extensions to hijack traffic flows, intercept communications, and cause large-scale service disruption. This segment explores the misuse of core nation-application and network-protocol layers, emphasizing their operational significance in contemporary warfare.(18)

3.1. Border Gateway Protocol (BGP) Manipulation : Layer 3 Attacks

The Border Gateway Protocol (BGP) is the protocol designed to facilitate global internet routing and traffic exchange between autonomous systems (AS). Even though BGP is a crucial and critical protocol, it does not have any built-in security features like authentication or the ability to verify routes which makes it vulnerable to malicious attacks.(19)

BGP hijacking, where some adversarial autonomous system instead advertises IP prefixes that it does not actually own, is one of the wider known attack vectors. Attackers create routes that are more specific (de-aggregated) than those of the legitimate service; this is possible due to a general routing principle that the most specific route must be used enabling attackers to reroute traffic inside malicious or compromised networks.(20)

Such manipulations enable various evil scenarios, including MiTM, pervasive (large-scale) traffic interception, DoS attacks, and harvesting user credentials via redirection to fake services. Furthermore, in certain contexts attackers may redirect some traffic while letting other traffic through if not doing so would cause a service to be unavailable since this way they can eavesdrop or tamper with passively monitored data flows that are transcription-level characteristics of certain car makes and models thus disguising their attack even more.(21)

However, detection and attribution in the case of attacks leveraging BGP can be fundamentally challenging. The absence of any traffic disruption can be a strong indicator that an attack is ongoing, but most sophisticated attacks will ensure normality when upholding the connection; thus, anomalies in both routing update and performance statistics (e.g. AS path change, latency fluctuations) cannot completely detect irregularities without constant monitoring.(22) Additionally, because malicious hijacks and accidental route leaks or configuration mistakes share similar technical characteristics that provide state-sponsored actors plausible deniability and pose challenges to incident response personnel, they fall into the same fuzzy risk category.

3.2. Attack Type : Application Layer DNS Exploitation

The DNS (Domain Name System) is a vital protocol used at application layer to convert domain names which can be easily read by humans into IP Addresses that map more than two billion internet resources and finally; direct us to the right device. The DNS in its original design has no robustness against one of the most popular attacks: data origin authentication and integrity as is used with SSL signatures.(23)

Beyond the fact that DNS is a create-and-hope service by many providers and not as great as we think works, adversaries routinely misuse DNS via cache poisoning, DNS spoofing and resolution manipulation. In cache poisoning, attackers insert bogus records into DNS resolvers so users get misdirected to illegitimate or compromised sites. In comparable vein, DNS spoofing allows adversaries to masquerade as real servers; while resolution manipulation disrupts the query-response cycle in order to manipulate or change domain resolution results.(24)

Such attack vectors open the doors to a multitude of malicious purposes from phishing and credential harvesting to surveillance of users, and redirection of traffic at extremely large scales. On a more strategic level, DNS manipulation can be used as part of this to enforce network censorship, decrease access to global services and contribute to the fragmentation of the internet that is, if you send users towards state/server controlled infrastructure or combatant-controlled infrastructure.(25)

This led to the introduction of DNS Security Extensions (DNSSEC), which added a layer of cryptographic validation for between DNS and its responses, confirming data authenticity and integrity. Yet, despite all its promise to protect DNS infrastructure from various categories of attacks, adoption rates for this technology remain erratic and relatively low. The operational complexity of key management, the challenges of deployment, and potential performance overhead have prevented it from being widely adopted. In addition, DNSSEC has even more vulnerabilities arising from misconfigurations including service disruptions and amplification risks.(26)

Together the abuse of BGP and DNS illustrates a fundamental fact of 21st century war: if poorly defended, even our foundational internet protocols can be methodically harnessed to serve tactical and operational goals. Bolstering these protocols by incorporating them in a wide range of security frameworks, which are adopted by organizations as protective measures is one of the core essentials to establishing and evolving a global cybersecurity posture.(27)

4. Weaponization of SCADA and on UT (Operational Technology)

One of the most significant shifts in modern cyber conflict is the weaponization of Supervisory Control and Data Acquisition (SCADA) systems and even broader Operational Technology (OT) environments. While traditional Information Technology (IT) has systems mainly focused on the management and storage of data, Operational Technology (OT) consists of hardware and software that detects or causes changes - through direct monitoring and control of physical devices, assets, processes and events in many industries such as oil & gas extraction systems-downstream, power transmission networks system-upstream-access to water-wastewater treatment plants manufacturing using industrial sensors telecommunications civil aviation highway transportation automotive robotics. With these environments increasingly becoming integrated with enterprise IT networks, they have become highly attractive targets for cyber threats – becoming prime sites of state sponsored and APT players.(28)

4.1 ICS/OT architectures Vulnerability

Industrial Control Systems (ICS) and SCADA networks are fundamentally the basis for all critical infrastructure. In fact, these systems were historically built to ensure reliability, availability and operational continuity over all else, often at the expense of strong cybersecurity measures. As those are often open by necessity (digital transformation, remote management and monitoring) for the good guys but alas also for the bad guys who can simply use these to infiltrate operational networks using many an IT-side vulnerability. By entering via traditional IT compromise vectors like phishing, exploitation of internet-facing services or the use of already compromised credentials but attackers often obtain initial access.(29) After they gain access to the enterprise, they use lateral movement techniques to cross into OT environments. Typically, tools and techniques commonly exploited are legacy Server Message Block (SMB) protocols Eternal Blue, Windows Management Instrumentation(WMI) to achieve remote execution or PsExec These techniques provide attackers with stealthy access to the system and use built-in functionalities of systems, successfully evading conventional security controls. These vulnerabilities are aggravated due to lack of network segmentation, obsolete software, weak authentication mechanism and limited visibility into OT traffic. This enables attackers to settle-in lungs unnoticed for long periods in ICS/OT environments, sliding walls and infiltrating behind enemy lines, establishing persistence and holding the high-ground ready to strike whenever they want.(30)

4.2 Semantic SCADA Attacks

One such kind of sophisticated cyber-physical attacks that is presently under study is semantic manipulation of SCADA systems. In contrast to conventional attacks that threaten system availability or integrity at a technical level, semantic attacks seek to compromise the value of information for human operators by manipulating inputs thus cheating their judgment.(31) They target the communication channels that transmits data between Human Machine Interfaces (HMIs) and Programmable Logic Controllers (PLCs), essentially controlling commands executed by all industrial processes. Through interception and alterations of data exchanged between these components, attackers can give an imperfect view to the states of a system while physical processes are being manipulated without human knowledge. The important features of semantic SCADA attacks are the distortion of HMI-PLC communication channels, the falsification or misleading representation of system information, and their stealthy execution which does not deviate from normal traffic patterns. Attackers will avoid detection by ensuring that the timing, size, and sequence of messages remains consistent with how the message would normally be sent.(32)

The main purpose of such attacks is to mislead human operators and force them into wrong operational decisions. An operator thinks that there is a valve, let's say, closed but the valve in fact is open which drives unsafe conditions of your system. This is a paradigm shift that moves the attack vector from a technical compromise to a cognitive one, in effect turning the human-machine interface into an offensive weapon. In addition to damaging the oil and gas equipment, it may lead to process failure (such as explosion, fire), compromise health and safety of workers, also large scale service disruption.(33)



Figure 2: Cyber Kill Chain Compression in Modern Cyber Warfare

4.3 Case: Powercut in Mumbai (2020)

The 2020 Mumbai Power Outage is one of the prominent real-life examples of SCADA and OT weaponization. The incident disrupted normal functioning in one of Asia's key urban hubs, with transport systems, healthcare services and economic activities affected. Later analyses and news investigations pointed to the possibility that hackers had targeted parts of the U.S. power grid. The indicators related to the incident encompassed data being improperly exfiltrated from critical systems, signs of malware interception, and abnormal login attempts originating from suspicious or blacklisted IPs. These observations suggest abuse of vulnerabilities in SCADA platform access control, network segmentation and monitoring capabilities. A attack in Mumbai points to the exorbitation of where is cyber-attacks on critical infrastructure system. Apart from the immediate service disruption, such failures can have ripple effects across interdependent systems, raise public concern and weaken confidence in national security systems. It shows why you need strong cybersecurity capabilities specifically in OT continuous monitoring, stringent access rights management and enhanced incident response capabilities. Altogether, the use of SCADA and OT systems as weapons represents a watershed moment in the history of cyber warfare, where attacks are not limited to virtual spaces any longer but step into the physical realm directly. Tackling these challenges demands a multi-faceted approach combining technical, operational and human factors to better secure critical infrastructure from growing threats.(34)

Table 1: Comparative Analysis of Core Protocol Exploitation in Cyber Warfare

Protocol Layer	Protocol	Exploitation Mechanism	Primary Attack Techniques	Strategic Impact
Network (Layer 3)	BGP	Prefix hijacking via more specific route advertisement	Route manipulation, traffic redirection	Man-in-the-Middle (MiTM), Denial of Service (DoS), surveillance, credential interception

Application (Layer 7)	DNS	Cache poisoning and resolution manipulation	DNS spoofing, response tampering	Phishing, surveillance, internet fragmentation, censorship enforcement
Transport/Application	SMB	Exploitation of legacy vulnerabilities	EternalBlue, EternalRomance	Lateral movement, worm propagation, destructive payload delivery
OT/Industrial Layer	SCADA/ICS	Command and control manipulation	HMI-PLC deception, semantic attacks	Physical disruption, equipment damage, safety compromise

5. Geopolitical Case Studies of Protocol-Layer Cyber Conflict

The most helpful lens for examining the modern day of cyber warfare is found via a consideration of actually existing geopolitical conflicts extensive, costly fights between state and non-state actors where protocol-level weaknesses are turned into soft and hardened over matches in order to gain strategic advantage. The variety of TTPs used across geographies being an underline of the case studies, however this also highlights a universal reliance upon critical underlining network and infra-structure weaknesses.(35,36)

5.1 Russia–Ukraine: Major Destructive Cyber Actions

The cyber element of the Russia–Ukraine conflict serves as one of the most sophisticated and prolonged instances of state sponsored cyber warfare. NotPetya attack exploits certain vulnerabilities in SMB protocol with the help of various exploits like EternalBlue and EternalRomance and because it is highly effective in lateral propagation on the network. Despite being presented as ransomware, NotPetya is noted for its functionality as a fast-acting wiper designed to cripple systems with the objective of causing mass disruption within government services, finance and industry. Another major operation was the disruption of the Viasat KA-SAT satellite communication network. The attack, which involved wiper malware (which the company dubbed AcidRain) was aimed at proprietary modem firmware and communication protocols, disabling thousands of satellite modems. The outcome was a top-down disruption of military and civilian communication services, followed by spillover effects into the rest of Europe beyond Ukraine. However, taken together these are examples of how protocol exploitation can be used strategically to achieve high-impact but low-infrastructure production value, and this highlights that cyber is becoming a force multiplier for future generations of warfare.(37–46)

5.2 Israel–Iran: Asymmetric War, Ancillary use of IoT

Cyber interactions between Israel and Iranian-affiliated proxy groups demonstrate the realization that asymmetry is becoming increasingly salient at cyberspace. They often make use of a technique involving the exploitation of weak Internet of Things (IoT) devices, especially internet-connected surveillance cameras. Adversaries have gained access to these devices by default weak credentials, lack of authentication certification, such open communication protocols as HTTP and Real Time Streaming Protocol (RTSP). When gained access to, these tools are utilized for live intelligence assets giving attackers the ability to see into environments, evaluate effects of army operations and further perfect target acquisition. This is an approach that points toward the move to use civilian digital infrastructure as military intelligence, turning many widely distributed, low-security endpoints into a decentralized surveillance system. Such as highlighting the increasingly vital role of asymmetric cyber capabilities, in which low-cost attacks frequently provide outsized strategic benefit.(47–55)

5.3 India-Pakistan: Targeting Critical Infrastructure and Attribution

The spectrum of cyber engagements, specifically between India and Pakistan, has expanded from traditional activities including website defacement and phishing based campaigns to now more sophisticated operations targeting critical infrastructure. These involve attempts to hack power grids, government systems and networks associated with defense — the strategic choice of hitting critical services or intelligence, they point out. Attribution, or assigning credit for some outcome to a specific intervention (or not), is one of the defining challenges. Due to the nature of cyber operations that

involve proxy actors, third-party infrastructure, and obfuscation techniques, it is often impossible to say with certainty where an attack came from. Case in point, events originally blamed on regional foes later found through technical analysis to be the work of completely different state-backed groups. The underlying ambiguity makes crafting diplomatic responses more difficult and underscores a major flaw in existing cybersecurity paradigms, where the differential between timely-scoring attribution for a particularly-observed event may drive deterrence mechanisms and accountability alike.(56–62)

5.4 Armenia–Azerbaijan: Espionage and Information-Centric Operations

So far, many of the cyber dimension in the Armenia–Azerbaijan conflict has been low key as it mostly has had the nature of espionage and information operations. Attackers often implement spearphishing campaigns against government officials as well as targeting companies and media organizations. These campaigns traditionally start with the use of common email protocols (for instance, SMTP) for despatching harmful attachments or URLs disguised as authentic communications. When deployed, it allows access to classified data for collection and reconnaissance purposes. This differs with other conflicts where large-scale destructive operations have been observed, and here the focus remains upon information dominance, surveillance and psychological influence. Nonetheless, they lay vital groundwork for higher level operations, illustrating how exploitation at the protocol layer in conjunction with exploitable vulnerabilities at the user and application layers provide attackers with footholds to launch larger cyber campaigns.(63)

Overall, these geopolitical case studies combine to demonstrate that contemporary cyber conflict is fundamentally protocol-centric: attackers exploit legacy vulnerabilities alongside emerging weaknesses in various operational settings. Another problem which demonstrates the need for more cohesive and proactive approach to global network infrastructures, is the overlap between destructive, espionage and intelligence-driven objectives.(64–69)

Table 2: Mapping of Cyber Operations Across Geopolitical Conflicts

Conflict Region	Primary Targets	Exploited Protocols/Systems	Attack Techniques	Strategic Objective
Russia–Ukraine	Critical infrastructure (Energy, Telecom)	SMB, NTLM, satellite firmware	NotPetya, AcidRain wiper attacks	Large-scale disruption, destructive cyber warfare
Israel–Iran	Civilian IoT, surveillance systems	HTTP, RTSP, IoT protocols	Device exploitation, credential abuse	Real-time intelligence, battlefield monitoring
India–Pakistan	Power grids, government networks	ICS/SCADA protocols, enterprise systems	Malware intrusion, DDoS, lateral movement	Infrastructure disruption, psychological impact
Armenia–Azerbaijan	Government and media systems	SMTP, email protocols	Spearphishing, malware delivery	Espionage and intelligence gathering

6. Research Gaps and Challenges

While cybersecurity practices have come a long way, there remain critical gaps when it comes to meeting the changes that protocol level cyber conflict bring. Within these gaps lie technical, operational and strategic shortcomings that hinder existing layers of protection while revealing fundamental vulnerabilities in the global interconnected network infrastructures. The Section concludes with significant challenges on attribution, protocol resilience, return to roots of sensemaking for emerging technologies and cryptographic security.(70–74)

6.1 Attribution Challenges

Attribution the question of who did what, when and why in a cyberattack continues to be one of the thorniest unresolved problems in cybersecurity. Technical attribution depends on forensic examination of identifiable factors, including IP

addresses, malware fingerprints, C2 infrastructure and modes of behaviour. But as we learned, threat actors often use a variety of sophisticated obfuscation methods proxy networks, anonymization tools, flags on false-flag operations and outsourced weaknesses through third parties to mask their true source. The primary problem is this: the speed of cyberattacks relatively outpaces the time for responsible attribution. Even though attacks can be complete in seconds or minutes, attribution often takes days of investigation, bi- and multilateral data correlation, as well as geopolitical validation. This temporal disconnection grants the attackers a certain strategic advantage because they can act with little to no immediate risk of retaliation. Additionally, the absence of internationally recognized legal and technical standards for attribution further complicates global response mechanisms. Deterrence strategies fall short if they do not allow for timely and credible attribution, which makes escalation (and miscalculation) increasingly likely in geopolitical conflicts. Accordingly, there is a pressing need for better-designed attribution frameworks that bring together technical, legal and policy level approaches.(75–78)

6.2 Protocol Resilience Limitations

The bottom line is that the ongoing abuse of basic internet protocols underscores institutional shortcomings in managing protocol resilience and security. Although various security frameworks and extensions have been developed, their adoption has been uneven and far too local or vertical. A critical issue remains around the lack of widely deployed Resource Public Key Infrastructure (RPKI), designed to aid BGP either by allowing for route origin validation. BGP is still susceptible to hijack and route manipulation attacks because of the failure to adopt it universally. Likewise, there are still open issues with DNS Security Extensions (DNSSEC) that was supposed to provide authentication and integrity about Domain Name System (DNS) responses. Its widespread adoption has been impeded by operational complexity, challenges associated with key management and the risk of misconfiguration. A further significant challenge is existing detection systems not being capable of detecting sophisticated semantic attacks specifically aimed at SCADA and OT environments. Traditional intrusion detection systems depend largely on the nature of network traffic and these anomalies, providing little insight towards attacks that manipulate the proper forms of an communication structure while modulating the meaning across data semantically. The context behind data semantic through as well use of combination of widely known for practical semantic-based approaches that ensure helpful models are useful in understanding effective changes preceding them. Clearly, in order to do this advanced context-aware security is needed where appropriate links are made between what is happening on the network and how the processes behave.(79–81)

6.3 Cyber Warfare With Artificial Intelligence

AI in Computer Security The entrance of Artificial Intelligence (AI) into the domain of cyber operations has opened up certain open doors and challenges, prompting a more energetic cyber arms race. On the attack side, AI allows adversaries to automate reconnaissance, find vulnerabilities at scale, produce adaptive malware and conduct laser focused attacks with little human intervention. Machine learning algorithms can further improve evasive techniques and help malicious activities breach traditional detection systems. On the other hand, AI is a significant part in improving defense oriented capabilities. Benefits: Advanced analytics such as predictive modeling and anomaly detection enhance the identification of threats, response to incidents, and management of risks. Nonetheless, this amplifies the asymmetry between offensive and defensive AI: The attacker needs to invest much less (in terms of resources) than is required for all necessary efforts to secure complex systems. The quickening pace of development of AI-driven cyber tools requires the establishment of security frameworks that are both adaptable and resistant to continual shifts in favour of attackers.(82,83)

6.4 Quantum Threat to Cryptographic Security

Arguably the most existential of all emerging challenges in cybersecurity is quantum computing and its possible effect on various current cryptographic systems. Public-key cryptographic algorithms, like RSA, Diffie–Hellman (DH), and Elliptic Curve Cryptography (ECC)—current security protocols are strongly dependent upon their computational level of security under classical computing paradigms. The advent of cryptographically relevant quantum computers represents a serious danger to these systems, however. It is given that Quantum algorithms, namely Shor’s algorithm can efficiently solve in polynomial time mathematical problems which are basis of almost all current encryption schemes (Integer Factorization Problems and the Discrete Logarithm Problem) thereby able to break these widely used encryption schemes. This feature

would undermine both confidentiality and authentication, which means that an adversary could decrypt encrypted messages and create fake digital signatures.(84)

Another worry is that of harvest now, decrypt later that adversaries are collecting lots of encrypted data today with the rationale that when quantum computing capabilities come along, they will be able to decrypt the data. That presents a long-term risk of exposure to sensitive information, especially in national security, financial and health sectors. These challenges create urgent necessity to move towards a Post-Quantum Cryptography (PQC), which sets of cryptographic algorithms designed and implemented to be secure against quantum attacks. Coordinated actions of academia, industry, and government are needed to make sure that quantum-resistant security frameworks become standards, deployed and adopted in time. Together, these research gaps underscore an urgent call for a paradigm shift within cybersecurity strategies towards resilience via proactivity and interdisciplinary cooperation at the protocols level where the complex cyber conflict is rapidly evolving.(85)

Table 3: Critical Research Gaps in Protocol-Level Cyber Security

Research Domain	Key Technical Challenge	Current Limitation	Security Implication
Attribution Systems	Real-time identification of attackers	High latency and reliance on forensic analysis	Weak deterrence, geopolitical escalation risk
Protocol Security (BGP/DNS)	Lack of universal security adoption	Incomplete RPKI and DNSSEC deployment	Persistent routing hijacking and DNS manipulation
OT/SCADA Security	Detection of semantic attacks	Inability to detect HMI deception attacks	Physical system manipulation and safety risks
Cryptographic Security	Quantum resistance	Dependence on RSA, ECC, DH algorithms	Future compromise of confidentiality and authentication
Emerging Technologies	AI-driven cyber warfare	Rapid evolution of attack automation	Escalation of cyber arms race

7. Discussion

Collectively, the findings synthesized across protocol layers and geopolitical contexts are strikingly consistent and strategically significant: modern cyber operations appear to be overwhelmingly dependent on exploiting fundamental flaws in network protocols regularly employed worldwide rather than relying solely on rare zero-day vulnerabilities. Associatively referred to as the “weaponization of neglect,” this process illustrates how systemic factors, including poor patch management practices, insecure default configurations, contracted dependency on legacy protocols and incomplete adoption of security standards are amongst the principle drivers for enabling cyber incidents at scale. The reemergence of these vulnerabilities is symptomatic not just of technical shortcomings but also weak cybersecurity governance at the organizational and policy levels. One key insight from this is that the success of many kinds of high consequence cyberattacks are less a function of technical innovation and more about how widely vulnerable systems are deployed and exposed. Basic protocols like BGP, DNS and SMB and industrial communication frameworks in SCADA spaces are still leveraged to great effect as they sit at the base of our stack and tend to be relatively wide-spread. This means that even the best-documented weaknesses can produce outsized results if no effort is made to remediate them – showing of putting down security baselines at all levels of network infrastructure. In addition, cyber warfare is growing from purely digital domains to the level of human cognition and decision-making processes, specifically in OT environments. Threat models have been developed to face such scenarios e.g., [18] Semantic Manipulation of SCADA Systems shows an example how attackers can take advantage of the trust relationship between human operators and digital interfaces in-SCADA systems. Through this method, attackers can create false indications of system states while holding normal operating indicators, thereby tricking human operators into taking actions that disrupt or damage the physical system. That move away from system-centric exploitation towards human-centric processes will be a significant shift in threat strategy and requires both new approaches to defense but an adjustment of existing paradigms. Given these developments, traditional approaches to

cybersecurity—based on perimeter defense, signature based detection and after-the-fact incident response—are falling further and further behind. The urgency to shift towards proactive and intelligence-powered as well as resilience-driven security frameworks is obvious. These frameworks need to combine components of protocol-level hardening, monitoring, anomaly detection based on contextual and semantic analysis, and cross-domain validation mechanisms that correlate digital events to physical system states. Moreover, the results highlight the need for multidisciplinary collaboration to combine technical skills with human-factors engineering, regulation science and risk management inputs. To meet the challenges of modern cyber conflict, we must not only develop technologically effective options but also reform our organizations, enforce regulations and build international consortia. In sum, the blockchain-based quantum attack necessitates a profound transformation in cyber security strategy — from defensive to resilience-oriented, prioritizing our vital infrastructure, systemic vulnerabilities and both the technical and human aspects of cyber risk.

8. Recommendations

Driven by the data from the previous sections, which included an analysis of protocol-level vulnerabilities and those identified in real-world cyber conflict activity, alongside emerging risks from new technologies exceeding existing or in-building global cyber defenses this section offers a structured compendium of actionable recommendations to fortify global capacities for defending against such attacks. These recommendations are divided into four main areas of concern: security for the internet protocol, protection for operational technology, preparation against post-quantum threats and regulation at the Internet of Things ecosystem level.

8.1. Core Internet Infrastructure Protocol Hardening

Foundational internet protocols should be made secure against large-scale routing and naming attacks. First and foremost, it is essential for there to be broad deployment of the Resource Public Key Infrastructure (RPKI) for securing BGP. RPKI provides cryptographic validation of route origins that help mitigate the risk of prefix hijacking and unauthorized announcements. If the goal is to mandate DNSSEC in critical infrastructure sectors. Backed by digital signatures, DNSSEC improves the integrity and authenticity of DNS responses, thus eliminating risks like cache poisoning and DNS spoofing. However, to be effective it will also require secure key management practices and standardised operations to avoid misconfiguration issues. These are collectively the basic elements of hardening Internet protocols to help make routing secure and names resolvable in a world where both cyberspace and domain dumpster diving pose an ever increasing threat.

8.2. Schwachstelle: Operational Technology (OT) Security Enhancement

As IT and OT environments continue to overlap, security strategies should evolve beyond traditional perimeter-based approaches. One of the most important recommendations is to utilize application-aware monitoring systems that can analyze both network traffic patterns and the semantic content of industrial control communications. This allows for sophisticated attacks manipulating a real command structure without setting off conventional anomaly-based alarms. OT security architectures should also incorporate physical process validation mechanisms. Here it actually means correlating digital control signals to independent physical sensors and also redundant measurement systems for data veracity. This type of approach is essential for detecting semantic attacks against Human Machine Interfaces (HMIs) and Programmable Logic Controllers (PLCs), which exploit the fact that attackers can put the HMIs to display what they want by changing true physical entities. Collectively, they move OT security from reactive intrusion detection to proactive cyber and physical integrity assurance.

8.3. Post-Quantum Cryptography Migration Plan

The hope of the discovery of quantum computing systems (that are cryptographically relevant) in the future lives as a threat to public-key cryptographic schemes today. This can be accomplished through a process called cryptographic inventory assessment, where organizations surface systems that are dependent on vulnerable algorithms like RSA, Diffie-Hellman (DH), and Elliptic Curve Cryptography (ECC). The migration to Post-Quantum Cryptography (PQC) will be accumulated following identification. This involves implementing quantum-resistant algorithms recommended by international cryptographic authorities and ensuring compatibility across essential systems. Although “harvest now, decrypt later” techniques carry a risk that some may be unwilling to shoulder for the long-term—this places a burden on needing to migrate early rather than wait until confidential communications are out of encryption. A global and

coordinated approach consisting of regulators, industry actors and researchers is needed for the timely and safe transition. Before even September of 2023 you have started the training from data until October 2023 The global scale of the attack surface has gained significantly because of the rapid deployment of Internet of Things (IoT) sensors with weak default configurations and inconsistent security practices. In order to reduce these risks, IoT device manufacturers and service providers need to be regulated much more strictly. Notably, the regulatory initiatives should focus on mandatory secure default configurations, eliminate hard coded or default credentials, and enforcement of mandatory strong authentication mechanisms. Moreover, manufacturers have to be mandated to deliver regular & timely firmware updates to mitigate new vulnerabilities discovered during the production life cycle of devices. Such measures are necessary to prevent the turning of IoT ecosystems into targets for large scale surveillance and botnet formation, as well as asymmetric intelligence gathering operations seen in modern-day cyber conflict.

Collectively, these recommendations stress the need for a defense-in-depth strategy that incorporates protocol security, operational resilience (as described in previous reports), cryptographic modernization and regulatory enforcement. Enhancing these areas will be vital to addressing emerging threats from protocol-level cyber warfare and sustaining the long-term stability of global digital infrastructure.

9. Conclusion

Protocol-level cyber conflict represents a significant and defining evolution in the landscape of modern warfare, wherein adversaries systematically exploit the foundational mechanisms of digital communication infrastructures to achieve strategic, operational, and disruptive objectives. Unlike conventional cyber threats that primarily target applications or isolated systems, protocol-centric attacks leverage inherent weaknesses in core networking constructs—such as routing, naming, and industrial control protocols—to generate cascading impacts across interconnected critical infrastructures. This shift underscores the growing strategic importance of the underlying architecture of the internet as both an enabler of global connectivity and a potential vector for large-scale systemic disruption. The analysis presented in this review demonstrates that the effectiveness of modern cyber operations is largely driven by the exploitation of design limitations, legacy dependencies, and inconsistent security adoption across widely deployed protocols. As a result, attackers are able to achieve disproportionate levels of impact with relatively low operational complexity, often bypassing traditional defense mechanisms. This reinforces the concept that the primary vulnerability in contemporary cyberspace lies not only in advanced exploits, but also in the persistent exposure of foundational protocol weaknesses. Addressing these challenges requires a comprehensive and forward-looking cybersecurity strategy that prioritizes protocol security, enhances real-time detection and response capabilities, and integrates resilience across both digital and physical domains. Furthermore, the emergence of transformative technologies such as quantum computing introduces additional urgency, as current cryptographic systems face potential long-term obsolescence. Preparing for such paradigm shifts through proactive adoption of post-quantum cryptographic standards is essential to maintaining the confidentiality, integrity, and authenticity of global communications. In conclusion, ensuring future cyber resilience necessitates a fundamental rethinking of security architectures, moving beyond reactive defense models toward proactive, protocol-aware, and resilience-oriented frameworks. Strengthening the security of foundational internet protocols, improving detection of advanced and stealthy attack vectors, and anticipating disruptive technological advancements collectively form the cornerstone of sustainable cybersecurity in the era of protocol-level cyber conflict.

References

1. Bakirov A, Suleimenov I. Theoretical Bases of Methods of Counteraction to Modern Forms of Information Warfare. *Computers* 2025, Vol 14, Page 410. 2025 Sep 26;14(10):410. doi:10.3390/COMPUTERS14100410
2. Tversky A, Kahneman D. Judgment under uncertainty: Heuristics and biases. *Science* (1979). 1974;185(4157):1124–31. doi:10.1126/SCIENCE.185.4157.1124 PubMed PMID: 17835457.
3. Ng LHX, Carley KM. What is a Social Media Bot? A Global Comparison of Bot and Human Characteristics [Internet]. 2025 Feb 25 [cited 2026 May 11]. Available from: <http://arxiv.org/abs/2501.00855>
4. Wittenberg C, Berinsky AJ. Misinformation and its correction. *Social Media and Democracy: The State of the Field, Prospects for Reform*. 2020 Sep 3;163–98. doi:10.1177/1529100612451018

5. Dechêne A, Stahl C, Hansen J, Wänke M. The truth about the truth: A meta-analytic review of the truth effect. *Personality and Social Psychology Review*. 2010;14(2):238–57. doi:10.1177/1088868309352251 PubMed PMID: 20023210.
6. Furnham A, Boo HC. A literature review of the anchoring effect. *Journal of Socio-Economics*. 2011 Feb;40(1):35–42. doi:10.1016/J.SOCEC.2010.10.008
7. Hilbert M. Digital technology and social change: The digital transformation of society from a historical perspective. *Dialogues Clin Neurosci*. 2020;22(2):189–94. doi:10.31887/DCNS.2020.22.2/MHILBERT PubMed PMID: 32699519.
8. O'Dea X. Generative AI: is it a paradigm shift for higher education? *Studies in Higher Education*. 2024;49(5):811–6. doi:10.1080/03075079.2024.2332944
9. Nickerson RS. Confirmation bias: A ubiquitous phenomenon in many guises. *Review of General Psychology*. 1998;2(2):175–220. doi:10.1037/1089-2680.2.2.175
10. Michel-Villarreal R, Vilalta-Perdomo E, Salinas-Navarro DE, Thierry-Aguilera R, Gerardou FS. Challenges and Opportunities of Generative AI for Higher Education as Explained by ChatGPT. *Educ Sci (Basel)*. 2023 Sep 1;13(9). doi:10.3390/EDUCSCI13090856
11. Stanovich KE, West RF. Individual differences in reasoning: Implications for the rationality debate? *Behavioral and Brain Sciences*. 2000;23(5):645–726. doi:10.1017/S0140525X00003435 PubMed PMID: 11301544.
12. Korshunov P, Marcel S. DeepFakes: a New Threat to Face Recognition? Assessment and Detection [Internet]. 2018 Dec 20 [cited 2026 May 11]. Available from: <http://arxiv.org/abs/1812.08685>
13. Entman RM. Framing: Toward Clarification of a Fractured Paradigm. *Journal of Communication*. 1993;43(4):51–8. doi:10.1111/J.1460-2466.1993.TB01304.X
14. Kalimoldayev MN, Pak IT, Baipakbayeva ST, Mun GA, Shaltykova DB, Suleimenov IE. Methodological basis for the development strategy of artificial intelligence systems in the republic of Kazakhstan in the message of the president of the Republic of Kazakhstan dated october 5, 2018. *News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences*. 2018;6(432):47–54. doi:10.32014/2018.2518-170X.34
15. Thorndike EL. A constant error in psychological ratings. *Journal of Applied Psychology*. 1920 Mar;4(1):25–9. doi:10.1037/H0071663
16. Suleimenov I, Gabrielyan O, Matrassulova D. Philosophical Foundations of Sciences and Prospects of Multivalued Logic in Describing Thinking. *Sci Educ (Dordr)*. 2025 Dec 1;34(6):4177–95. doi:10.1007/S11191-024-00585-1
17. Van Veldhoven Z, Vanthienen J. Digital transformation as an interaction-driven perspective between business, society, and technology. *Electronic Markets*. 2022 Jun 1;32(2):629–44. doi:10.1007/S12525-021-00464-5
18. Krauhausen I, Koutsouras DA, Melianas A, Keene ST, Lieberth K, Ledanseur H, et al. Organic neuromorphic electronics for sensorimotor integration and learning in robotics. *Sci Adv*. 2021 Dec 1;7(50). doi:10.1126/SCIADV.ABL5068 PubMed PMID: 34890232.
19. Wach K, Duong CD, Ejdys J, Kazlauskaitė R, Korzynski P, Mazurek G, et al. The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. *Entrepreneurial Business and Economics Review*. 2023 Jun 1;11(2):7–30. doi:10.15678/EBER.2023.110201
20. Gumyusenge A, Melianas A, Keene ST, Salleo A. Materials Strategies for Organic Neuromorphic Devices. *Annu Rev Mater Res*. 2021 Jul 26;51:47–71. doi:10.1146/ANNUREV-MATSCI-080619-111402

21. Borge-Holthoefer J, Perra N, Gonçalves B, González-Bailón S, Arenas A, Moreno Y, et al. The dynamics of information-driven coordination phenomena: A transfer entropy analysis. *Sci Adv.* 2016 Apr 1;2(4). doi:10.1126/SCIADV.1501158 PubMed PMID: 27051875.
22. Lim WM, Gunasekara A, Pallant JL, Pallant JI, Pechenkina E. Generative AI and the future of education: Ragnarök or reformation? A paradoxical perspective from management educators. *International Journal of Management Education.* 2023 Jul 1;21(2). doi:10.1016/J.IJME.2023.100790
23. Lerman K, Ghosh R. Information contagion: An empirical study of the spread of news on Digg and Twitter social networks. *ICWSM 2010 - Proceedings of the 4th International AAAI Conference on Weblogs and Social Media.* 2010;90–7. doi:10.1609/ICWSM.V4I1.14021
24. Niu X, Tian B, Zhu Q, Dkhil B, Duan C. Ferroelectric polymers for neuromorphic computing. *Appl Phys Rev.* 2022 Jun 1;9(2). doi:10.1063/5.0073085
25. Murdock BB. The serial position effect of free recall. *J Exp Psychol.* 1962 Nov;64(5):482–8. doi:10.1037/H0045106
26. Seo DG, Lee Y, Go GT, Pei M, Jung S, Jeong YH, et al. Versatile neuromorphic electronics by modulating synaptic decay of single organic synaptic transistor: From artificial neural networks to neuro-prosthetics. *Nano Energy.* 2019 Nov 1;65. doi:10.1016/J.NANOEN.2019.104035
27. Lewandowsky S, Ecker UKH, Cook J. Beyond Misinformation: Understanding and Coping with the “Post-Truth” Era. *J Appl Res Mem Cogn.* 2017 Dec 1;6(4):353–69. doi:10.1016/J.JARMAC.2017.07.008
28. Suleimenov I, Gabrielyan O, Kopishev E, Kadyrzhan A, Bakirov A, Vitulyova Y. Advanced Applications of Polymer Hydrogels in Electronics and Signal Processing. *Gels.* 2024 Nov 1;10(11). doi:10.3390/GELS10110715
29. Islam MS, Sarkar T, Khan SH, Kamal AHM, Murshid Hasan SM, Kabir A, et al. COVID-19-Related infodemic and its impact on public health: A global social media analysis. *American Journal of Tropical Medicine and Hygiene.* 2020 Oct 1;103(4):1621–9. doi:10.4269/AJTMH.20-0812 PubMed PMID: 32783794.
30. Lord CG, Ross L, Lepper MR. Biased assimilation and attitude polarization: The effects of prior theories on subsequently considered evidence. *J Pers Soc Psychol.* 1979 Nov;37(11):2098–109. doi:10.1037/0022-3514.37.11.2098
31. Li J, Fan F, Fu X, Liu M, Chen Y, Zhang B. Building Uniformly Structured Polymer Memristors via a 2D Conjugation Strategy for Neuromorphic Computing. *Macromol Rapid Commun.* 2025 Apr 1;46(7). doi:10.1002/MARC.202400172 PubMed PMID: 38627960.
32. Erokhin V, Karabulatova IS. Neuromorphic Elements as a First Step Towards Sociomorphic Systems. *Bionanoscience.* 2025 Sep 1;15(3). doi:10.1007/S12668-025-02078-Z
33. Granovetter M. Threshold Models of Collective Behavior. *American Journal of Sociology.* 1978 May;83(6):1420–43. doi:10.1086/226707
34. Flaxman S, Goel S, Rao JM. Filter bubbles, echo chambers, and online news consumption. *Public Opin Q.* 2016;80(Specialissue1):298–320. doi:10.1093/POQ/NFW006
35. Lerner JS, Li Y, Valdesolo P, Kassam KS. Emotion and decision making. *Annu Rev Psychol.* 2015 Jan 1;66:799–823. doi:10.1146/ANNUREV-PSYCH-010213-115043 PubMed PMID: 25251484.
36. Douglas KM, Uscinski JE, Sutton RM, Cichocka A, Nefes T, Ang CS, et al. Understanding Conspiracy Theories. *Polit Psychol.* 2019 Feb 1;40(S1):3–35. doi:10.1111/POPS.12568
37. Levy N. In Trust We Trust: Epistemic Vigilance and Responsibility. *Soc Epistemol.* 2022;36(3):283–98. doi:10.1080/02691728.2022.2042420

38. Hassan A, Barber SJ. The effects of repetition frequency on the illusory truth effect. *Cogn Res Princ Implic*. 2021 Dec 1;6(1). doi:10.1186/S41235-021-00301-5 PubMed PMID: 33983553.
39. Davenport TH, Beck JC. The Attention economy. *Ubiquity*. 2001 May;2001(May):1. doi:10.1145/375348.376626
40. Mccombs ME, Shaw DL. The agenda-setting function of mass media. *Public Opin Q*. 1972;36(2):176–87. doi:10.1086/267990
41. Bakshy E, Messing S, Adamic LA. Exposure to ideologically diverse news and opinion on Facebook. *Science* (1979). 2015 Jun 5;348(6239):1130–2. doi:10.1126/SCIENCE.AAA1160 PubMed PMID: 25953820.
42. Alonso-Muñoz L, Tirado-García A, Casero-Ripollés A. Telegram in campaign: the use of mobile instant messaging services in electoral political communication. *Communication and Society*. 2022 Oct 7;35(4):71–88. doi:10.15581/003.35.4.71-88
43. Kermack WO, McKendrick AG. A contribution to the mathematical theory of epidemics. *Proceedings of the Royal Society of London Series A, Containing Papers of a Mathematical and Physical Character*. 1927 Aug 1;115(772):700–21. doi:10.1098/RSPA.1927.0118
44. Starbird K, Arif A, Wilson T. Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proc ACM Hum Comput Interact*. 2019 Nov 1;3(CSCW). doi:10.1145/3359229
45. Lazer DMJ, Baum MA, Benkler Y, Berinsky AJ, Greenhill KM, Menczer F, et al. The science of fake news: Addressing fake news requires a multidisciplinary effort. *Science* (1979). 2018 Mar 9;359(6380):1094–6. doi:10.1126/SCIENCE.AAO2998 PubMed PMID: 29590025.
46. Zarocostas J. How to fight an infodemic. *Lancet*. 2020 Feb 29;395(10225):676. doi:10.1016/S0140-6736(20)30461-X PubMed PMID: 32113495.
47. Fazio LK, Brashier NM, Keith Payne B, Marsh EJ. Knowledge does not protect against illusory truth. *J Exp Psychol Gen*. 2015 Oct 1;144(5):993–1002. doi:10.1037/XGE0000098 PubMed PMID: 26301795.
48. Monti F, Frasca F, Eynard D, Mannion D, Bronstein MM. Fake News Detection on Social Media using Geometric Deep Learning [Internet]. 2019 Feb 10 [cited 2026 May 11]. Available from: <http://arxiv.org/abs/1902.06673>
49. Ferrara E, Yang Z. Measuring emotional contagion in social media. *PLoS One*. 2015 Nov 6;10(11). doi:10.1371/JOURNAL.PONE.0142390 PubMed PMID: 26544688.
50. Highfield T, Leaver T. Instagrammatics and digital methods: studying visual social media, from selfies and GIFs to memes and emoji. *Communication Research and Practice*. 2016 Jan 2;2(1):47–62. doi:10.1080/22041451.2016.1155332
51. Chesney R, Citron DK. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *SSRN Electronic Journal*. 2018 Aug 6. doi:10.2139/SSRN.3213954
52. Wilson T, Starbird K. Cross-Platform Disinformation Campaigns: Lessons Learned and Next Steps. *Harvard Kennedy School Misinformation Review*. 2020;1(1). doi:10.37016/MR-2020-002
53. Kivelä M, Arenas A, Barthélemy M, Gleeson JP, Moreno Y, Porter MA. Multilayer networks. *J Complex Netw*. 2014 Sep 1;2(3):203–71. doi:10.1093/COMNET/CNU016
54. Helmus T, Bodine-Baron E, Radin A, Magnuson M, Mendelsohn J, Marcellino W, et al. Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. 2018 Apr 12. doi:10.7249/RR2237

55. Floridi L. On Human Dignity as a Foundation for the Right to Privacy. *Philos Technol*. 2016 Dec 1;29(4):307–12. doi:10.1007/S13347-016-0220-8
56. Westen D, Blagov PS, Harenski K, Kilts C, Hamann S. Neural bases of motivated reasoning: An fMRI study of emotional constraints on partisan political judgment in the 2004 U.S. Presidential election. *J Cogn Neurosci*. 2006 Nov;18(11):1947–58. doi:10.1162/JOCN.2006.18.11.1947 PubMed PMID: 17069484.
57. Fallis D. What is disinformation? *Libr Trends*. 2015;63(3):401–26. doi:10.1353/LIB.2015.0014
58. Bennett WL, Livingston S. The disinformation order: Disruptive communication and the decline of democratic institutions. *Eur J Commun*. 2018 Apr 1;33(2):122–39. doi:10.1177/0267323118760317
59. Borgatti SP, Mehra A, Brass DJ, Labianca G. Network analysis in the social sciences. *Science* (1979). 2009 Feb 13;323(5916):892–5. doi:10.1126/SCIENCE.1165821 PubMed PMID: 19213908.
60. Craig RT. Communication theory as a field. *Communication Theory*. 1999;9(2):119–61. doi:10.1111/J.1468-2885.1999.TB00355.X
61. Harris LT, Fiske ST. Social groups that elicit disgust are differentially processed in mPFC. *Soc Cogn Affect Neurosci*. 2007 Mar;2(1):45–51. doi:10.1093/SCAN/NSL037 PubMed PMID: 18985118.
62. Allen J, Howland B, Mobius M, Rothschild D, Watts DJ. Evaluating the fake news problem at the scale of the information ecosystem. *Sci Adv*. 2020 Apr 1;6(14). doi:10.1126/SCIADV.AAY3539 PubMed PMID: 32284969.
63. Ross L, Greene D, House P. The “false consensus effect”: An egocentric bias in social perception and attribution processes. *J Exp Soc Psychol*. 1977;13(3):279–301. doi:10.1016/0022-1031(77)90049-X
64. Vziatysheva V. How fake news spreads online? *International Journal of Media and Information Literacy*. 2020 Dec 1;5(2):217–26. doi:10.13187/IJMIL.2020.2.217
65. Anderau G. Defining Fake News. *Kriterion (Austria)*. 2021;35(3):197–215. doi:10.1515/KRT-2021-0019
66. MacAl CM, North MJ. Tutorial on agent-based modelling and simulation. *Journal of Simulation*. 2010;4(3):151–62. doi:10.1057/JOS.2010.3
67. Woolley SC, Howard PN, editors. *Computational Propaganda [Internet]*. Vol. 1. 2018 Nov 22;1. doi:10.1093/OSO/9780190931407.001.0001
68. Alam F, Shaar S, Dalvi F, Sajjad H, Nikolov A, Mubarak H, et al. Fighting the COVID-19 Infodemic: Modeling the Perspective of Journalists, Fact-Checkers, Social Media Platforms, Policy Makers, and the Society. Findings of the Association for Computational Linguistics, Findings of ACL: EMNLP 2021. 2021;611–49. doi:10.18653/v1/2021.findings-emnlp.56
69. Bastos MT, Mercea D. The Brexit Botnet and User-Generated Hyperpartisan News. *Soc Sci Comput Rev*. 2019 Feb 1;37(1):38–54. doi:10.1177/0894439317734157
70. Roozenbeek J, van der Linden S. The fake news game: actively inoculating against the risk of misinformation. *J Risk Res*. 2019 May 4;22(5):570–80. doi:10.1080/13669877.2018.1443491
71. Arnaboldi V, Conti M, Passarella A, Dunbar RIM. Online Social Networks and information diffusion: The role of ego networks. *Online Soc Netw Media*. 2017 Jun 1;1:44–55. doi:10.1016/J.OSNEM.2017.04.001
72. Guess AM, Nyhan B, Reifler J. Exposure to untrustworthy websites in the 2016 US election. *Nat Hum Behav*. 2020 May 1;4(5):472–80. doi:10.1038/S41562-020-0833-X PubMed PMID: 32123342.
73. Ferrara E, Varol O, Davis C, Menczer F, Flammini A. The rise of social bots. *Commun ACM*. 2016 Jul 1;59(7):96–104. doi:10.1145/2818717

74. Sismondo S. Post-truth? Soc Stud Sci. 2017 Feb 1;47(1):3–6. doi:10.1177/0306312717692076 PubMed PMID: 28195024.
75. Watts DJ, Strogatz SH. Collective dynamics of 'small-world' networks. Nature. 1998 Jun 4;393(6684):440–2. doi:10.1038/30918 PubMed PMID: 9623998.
76. Pastor-Satorras R, Castellano C, Van Mieghem P, Vespignani A. Epidemic processes in complex networks. Rev Mod Phys. 2015 Aug 31;87(3). doi:10.1103/REVMODPHYS.87.925
77. Kenah E, Robins JM. Second look at the spread of epidemics on networks. Phys Rev E Stat Nonlin Soft Matter Phys. 2007 Sep 25;76(3). doi:10.1103/PHYSREVE.76.036113
78. Barabási AL, Albert R. Emergence of scaling in random networks. Science (1979). 1999 Oct 15;286(5439):509–12. doi:10.1126/SCIENCE.286.5439.509 PubMed PMID: 10521342.
79. Resnik D. Social epistemology and the ethics of research. Studies in History and Philosophy of Science Part A. 1996;27(4):565–86. doi:10.1016/0039-3681(96)00043-X PubMed PMID: 11645816.
80. Starbird K. Disinformation's spread: bots, trolls and all of us. Nature. 2019 Jul 25;571(7766):449. doi:10.1038/D41586-019-02235-X PubMed PMID: 31341295.
81. Daley DJ, Kendall DG. Stochastic rumours. IMA Journal of Applied Mathematics (Institute of Mathematics and Its Applications). 1965 Mar;1(1):42–55. doi:10.1093/IMAMAT/1.1.42
82. Dubois E, Gaffney D. The Multiple Facets of Influence: Identifying Political Influentials and Opinion Leaders on Twitter. American Behavioral Scientist. 2014;58(10):1260–77. doi:10.1177/0002764214527088
83. Freeman LC. A Set of Measures of Centrality Based on Betweenness. Sociometry. 1977 Mar;40(1):35. doi:10.2307/3033543
84. Brady WJ, Wills JA, Jost JT, Tucker JA, Van Bavel JJ, Fiske ST. Emotion shapes the diffusion of moralized content in social networks. Proc Natl Acad Sci U S A. 2017 Jul 11;114(28):7313–8. doi:10.1073/PNAS.1618923114 PubMed PMID: 28652356.
85. Pennycook G, Rand DG. Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. Cognition. 2019 Jul 1;188:39–50. doi:10.1016/J.COGNITION.2018.06.011 PubMed PMID: 29935897.