Leiden University Press

Chapter Title: The Critical State of Cyberspace
Chapter Author(s): Hans-Dieter Hiep

Book Title: Advances in Anti-Access and Area Denial (A2/AD)
Book Subtitle: From Defensive Technologies to A Whole-of-Society Approach
Book Editor(s): Edwin Dado, René Janssen, Roy Hamans, Marc Gouw, Kerry Malone
Published by: Leiden University Press. (2026)
Stable URL: https://www.jstor.org/stable/jj.40494811.19

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at https://about.jstor.org/terms



This book is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License (CC BY-NC-ND 4.0). To view a copy of this license, visit https://creativecommons.org/licenses/by-nc-nd/4.0/. Funding is provided by Leiden University Press.



*Leiden University Press* is collaborating with JSTOR to digitize, preserve and extend access to *Advances in Anti-Access and Area Denial (A2/AD)*

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

CHAPTER 13

# The Critical State of Cyberspace

*Hans-Dieter Hiep*

**Abstract**

NATO is currently in a 'grey zone':[1] increasingly being challenged in cyberspace while unable to attribute attacks, thus failing to deter. Simultaneously, many governments, businesses, and populations depend on the Internet and the cloud to function properly. This is a dangerous situation, since global Internet connectivity could get disrupted and destabilised.[2] This chapter explains the basic principles from an overall technological perspective, and discusses the challenge of anti-access and area denial (A2/AD) in the context of global Internet disruptions. What is the contested area, what are possible effects, and can those effects be limited? Using a layered approach, we define the cyber 'high ground' as maintenance of and control over critical infrastructure, from core to edge, from hardware to software. To ensure each cyber 'area' can be protected in isolation but still allow global cooperation, we argue it is important to control which paths data takes in the network, similar to air traffic control. This requires a new approach to organisation: we discuss a decentralised architecture for cyberspace, and how the Internet can be structured using federated networks, featuring geofencing and effect isolation, that has the potential to radically change the future of cyber warfare.

**Keywords**: Internet; Cloud; Control plane; Disruption; Reset; Decentralisation

## Introduction

### *Background*

The Internet (originally called the ARPAnet) is a fruit of DARPA. J.C.R. Licklider, DARPA's 1961 director of the Command and Control Research Office (later the Information Processing Techniques Office), envisioned how 'man-computer symbiosis'[3] could form networks of intellectual communities where artificially intelligent agents help humans process information, to support military data acquisition, internal communications, and decision making. Technically, unlike earlier telephone circuit-switched networks, ARPAnet deployed the first wide-area packet-switched network in 1969.[4] It economically supported 'bursty' data exchange, where at unpredictable moments lots of data is sent in a short time span. In the

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

older telephone network this pattern was costly or slow: it required allocating expensive trunk lines that stayed idle most of the time,[5] or setting up a circuit only when enough data accumulated thus increasing latency. ARPAnet also aimed for interoperability: connecting computers from many vendors at many sites, varying in computer architectures and operating systems.

One application was the Worldwide Military Command and Control System (WWMCCS).[6] The WWMCCS Intercomputer Network (WIN) initially used the telephone network, but there were worries about disruption when the central telephone offices could come under coordinated attack.[7] ARPAnet provided a backup network and selected the TCP/IP technology. Related technologies, such as packet radio, were further developed by DARPA. Development cost was about 150 million USD (in 1990 currency).

Eventually ARPAnet split into two parts. One part, NSFnet, grew to connect worldwide research and academic institutes. It was decommissioned and fully commercialised in 1995, forming today's Internet. The other part grew into the U.S. military network MILNET. In 1990 the security architecture for MILNET was updated, and it was noted that "the Internet is international and is only loosely managed through cooperation of its users. No central authority exists to make or enforce security rules."[8] Nonetheless, the Internet community made best-effort improvements, e.g. to support e-commerce and banking, but the scope was limited. Since 1986 the Internet Engineering Task Force (IETF) has acted as an international standards body based on 'rough consensus,' joining the Internet Society (ISOC) in 1993. Both organisations rely on volunteers and lack formal accountability for ensuring privacy and security, so it is unreasonable to expect that the commercialised Internet's underlying technologies were designed to protect against adversaries in cyber or cognitive warfare.

That the Internet aimed for interoperability facilitated its global spread. Early global applications were information systems, such as the World Wide Web developed at CERN, used by librarians and academics at connected universities and laboratories to maintain a global intellectual community. Over three decades, many applications have been built on top, ranging from e-commerce and banking to multimedia streaming, entertainment, and government services, all dependent on a functioning Internet. While the Internet community pursued permissionless innovation, numerous downsides have emerged from connecting mass populations. Harmful applications,[9] possibly more addictive than illegal substances and hard drugs,[10] illustrate why we must speak of 'users.'

The Internet is not only an addictive playground: in decades it has become a new battleground. Humans can be micro-targeted during psychological and cognitive manipulation operations,[11] and societies face viral misinformation[12] that fuels discord and polarisation.[13] Without mass populations connected, these

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

effects would be smaller and more manageable. Individual profiling and fine-grained tracking enable targeted cognitive effects, essential to fifth-generation warfare and grey-zone conflict.[14] The current Internet architecture lets non-state actors gain substantial control over cyberspace, allowing them to influence foreign states by manipulating politicians and civil servants:[15] some view this as a threat to democracy.[16] Authoritarian regimes also use the Internet for social control, exemplified by Iranian shutdowns,[17] while European democracies employ shutdowns to suppress independence movements.[18] Emerging risks include disruptions by digital Luddites.[19] All this serves as preparation for future sixth-generation warfare, 'which targets technical systems to possibly collapse a society through strategic sabotage.'[20]

*Motivation & Plan of the Chapter*

Since there is no central Internet authority and cyber-attacks are difficult to attribute,[21] disruptions can occur without anyone being held responsible. Adversaries can coordinate attacks that destabilise and disrupt the Internet, locally or globally. This risk defines the 'critical state of cyberspace,' motivating us to address current shortcomings and explore technologies and methods to improve the status quo.

A lack of control in critical networks and a lack of high-assurance computer technology exposes Europe to societal instability crises (cf. sixth-generation warfare).[22] Gartner and NLnet Foundation highlighted this early in their 2018 Next Generation Internet report:[23] "Every technical primitive from the current Internet must be re-evaluated against the full threat catalogue, as we cannot afford our multi-trillion euro economies and societies to not be able to trust the Internet as we move forward." Economies and societies want to trust the Internet: Can this trust be justified, and how can we design computers and networks to ensure true quality and justifiable trust?

Disruption attacks pose a significant national security threat. Adversaries, from lone 'hacktivists' to well-organised state actors, can jeopardise sovereignty by forcing governments to act, under the threat of a nation-wide or even global Internet kill switch that disturbs routing information so severely that many sites and services become unreachable.[24] One could call this attack 'ransomware of the higher-order.' These attacks can be viewed as an anti-access/area-denial challenge, as discussed in the second section.

The complexity of cyberspace is vast: the global state space includes all electromagnetic waves in transmission lines and electronic/photonic circuitry[25] used to exchange or process information. To get a sense of scale, the Internet currently transports zettabytes per year, and is projected to move about one yottabyte by 2030 via roughly 200 billion connections.[26] Constructing a single system to control and

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

secure the entire Internet seems therefore impossible and undesirable. Because sensors and actuators connect cyberspace with the physical world, many hybrid interactions arise: cyber-physical,[27] cyber-biological,[28] cyber-psychological,[29] and cyber-neural systems.[30] First-order effects in cyberspace produce indirect second-order cybernetic effects on these hybrid systems, showing the importance to maintain the 'high ground'.[31] Without control, arbitrary (malicious) actors could manipulate such hybrid systems. In a military context, such second-order effects include weapon system manipulation and even remote firing. We discuss the layered approach of control, and the role of formal methods in high-assurance computing and networking, in the third section.

More concretely, we can illustrate the critical state of cyberspace with several hacks. The Iranian hack of DigiNotar compromised a cryptographic authority, jeopardising the security of large parts of the Internet:[32] a single hack has global impact. Another example involves Europe's Internet backbone.[33] Internet eXchange Points (IXPs) and transit providers increasingly automate maintenance centrally via Software-Defined Networking (SDN).[34] An adversary controlling such a system could deploy configuration changes to hundreds of border routers simultaneously. In 2017 the author discovered a critical vulnerability in one of the world's largest Internet exchanges that could grant this level of control. Due to vulnerabilities in the Border Gateway Protocol (BGP), such access enables dissemination of false routing information globally, thereby disrupting Internet service providers worldwide. In the military context, these disruptions must be handled with resilience, what prof. K. Guttieri calls "fighting through disruption."[35] In the fourth section the BGP-controlled Internet and its weaknesses will be discussed.

A remedy is to connect vital sectors (finance, healthcare, energy, transportation, industry, defence, and education) to secondary 'backup' networks with a more secure architecture featuring failure isolation and geofencing. Technically, SCION (Scalability, Control, and Isolation On Next-generation networks)[36] is a clean-slate, high-assurance networking architecture with formally verified standards, protocols, and open-source reference implementation. It has reached production-grade software quality and is now entering the special-purpose hardware development phase. By adopting this federated architecture, keeping it separate from the current Internet while deploying Isolation Domains (ISDs), the attack surface can be significantly reduced, creating a 'galvanically isolated' higher ground – a protected network accessible only to verifiably trusted parties. The practical, policy, and doctrinal implications are discussed in the fifth section.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

### Anti-Access and Area Denial

We first examine the Internet from an anti-access and area-denial (A2/AD) perspective.[37] Anti-access refers to long-range prevention of forces entering a theatre, while area-denial refers to short-range restriction of freedom of action, confining operations to areas under adversarial control.[38] We focus on the physical and virtual layers of Grant's model of cyberspace,[39] omitting the cognitive layer. Grant's model is geographical, since cyber overlaps with all physical military domains: an 'area' of cyberspace encompasses all computing and communication technologies within its geographic bounds.

Existing Internet infrastructure enables rapid military deployment and connection to remote sensors/actuators: dense coverage lets forces operate outside established bases without building new communication networks (e.g. for command and control). In peace time those same networks serve civilian purposes. However, adversaries can disrupt this dual-use infrastructure to create anti-access effects: while forces can still physically enter a theatre, they cannot use disrupted communication networks and remote cloud computation. Consequently, commanders lose the ability to coordinate forces and must resort to other, more restricted means of communication. Disruption can also isolate already deployed forces, cutting off communication back home. When this occurs, secondary ad-hoc networks need to be deployed, since repairing the primary networks can be time consuming without the guarantee of restoring full control.

Internet infrastructure ranges from the core to the edge. The core consists of Internet eXchange Points (IXPs) and the backbone networks linking them. The edge includes local Internet Service Providers (ISPs) delivering last-mile connectivity (including 4G/5G/6G[40]), data centres operated by Managed Service Providers (MSPs) hosting services such as video conferencing, e-mail, file exchange, calendars, et cetera. Today, top-ranking IXPs can process 20 terabit per second,[41] and state-of-the-art backbone links reach 10 terabit per second.[42] This traffic traverses the *data plane*, where regular data flows occur. IXPs enable reachability across most of the Internet, a phenomenon known as the 'flat Internet'.[43] On top we have the *control plane*: the structures, including remote access and control systems, that maintain and support core infrastructure.

In flat networks, disruptions near the core have a larger impact. Consequently, core infrastructure is a high-value target,[44] making targeted reconnaissance and surveillance operations strategically attractive to adversaries. The control plane is indirectly a high-value target.[45] Jackpot is a centralised control plane that remotely manages many core infrastructure sites. When vital sectors and military operations rely on Internet connectivity, disruptions can cause second-order effects, such as energy-distribution problems or disrupted logistics of goods. In flat networks, a

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

single successful cyber operation against such a centralised control plane not only can produce a large first-order impact, but the impact is also amplified if cascading second-order failures are coordinated with other effects in the physical military domains.

Summarising the anti-access/area-denial challenge, the 2020s Internet mirrors the 1960s telephone network before ARPAnet was deployed as a backup: today IXPs take the place of the former central offices in the telephone network. Coordinated attacks on IXPs could result in loss of communication with new and existing force deployments, and can have significant economic, social, and political consequences.

Thus arises the question: When is an area of cyberspace 'red' (in control of an adversary), 'grey' (unknown or neutral), or 'blue' (under control by an ally)? What kind of effects can be generated when in control over IXPs? We follow the offensive cyber operation actions, as part of Grant's model,[46] referring to the (unclassified) JP 3-12 from the U.S. Department of Defence:[47]

- **Deny**: To prevent access to, operation of, or availability of a target function by a specified level for a specified time. In our case, the target function is Internet connectivity. Deny is sub-divided into:
  - **Degrade**: To deny access to, or operation of, a target to a level represented as a percentage of capacity for a period of time. Level of degradation is specified. In our case, this means less traffic passes, or specifically only some filtered traffic passes.
  - **Disruption**: To completely but temporarily deny access to, or operation of, a target for a period of time. Can be considered a special case of Degrade, which denies everything. In our case, this amounts to traffic black-holing: all traffic that passes through the IXP is to be dropped, effectively reducing the capacity of the overall network.
  - **Destroy**: To completely and irreparably deny access to, or operation of, a target. Destruction maximises the time and amount of denial. In our case, configurations could be changed to cause physical damage to the underlying supporting hardware.
- **Manipulate**: To control or change information, information systems, and/or networks. It uses an adversary's information resources to create effects not immediately apparent. The targeted network may appear to operate normally until secondary or tertiary effects, including physical effects, reveal evidence. In our case, this means changing route information and information flows (more technical details in the fourth section).

As soon as an adversary can achieve the above effects, the infrastructure is no longer under control of an ally: it is 'red'. Since an adversary may be able to achieve the above effects but does not wish to reveal this, we have the 'grey' area: the

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

contested area. We define the area of cyberspace to be 'grey' when there are risks or uncertainties as to whether the target function is and will remain functional at times when demanded. When evidence is found that the area was (likely) under control of an adversary, the 'grey' area may reveal itself to be 'red' after all.

If an ally can achieve the above effects it does not imply the infrastructure is considered under control, and thus 'blue'. An area is only 'blue' when it is reasonably certain it is neither 'grey' nor 'red', thus denying adversaries the possibility to achieve the above effects. This can only be proven by obtaining evidence about the quality of the critical components within a cyber area (publicly auditable, up to reasonable assumptions): this is the main goal of defensive cyber operations.[48]

Infrastructure and networks constantly change, making it hard to detect adversarial control. Adversaries infiltrate critical Internet infrastructure: entering via outer networks and reconfiguring software/firmware for persistence, so-called Advanced Persistent Threats (APTs).[49] Also hardware supply chain attacks, providing components with covert flaws (hardware Trojans), can compromise operating system security.[50] Risks and uncertainties about device quality are difficult to measure quantitatively. When infrastructure in commercial ISPs or IXPs contains APTs, the network appears functional for many years while still being vulnerable to an adversarial strike: attackers can exploit zero-day vulnerabilities, bypassing cyber defences that rely on invalid assumptions about the underlying technology.

As mentioned above, an area is uncontested only when adversarial action is impossible. This requires full knowledge of the hardware/software stack, its functional dependencies, expected behaviour, and various degrees in which the system can be provably correct. Correctness here is not 'perfect', it merely aims to explain complex systems as simply as possible, and prove that the simplified explanation exactly reflects reality. Two guiding principles to achieve this are: the extended Kerckhoff principle, and the elimination-of-complexity principle.

- The extended Kerckhoff principle requires a system to be secure, even if an adversary knows its internal workings. Applying it to critical infrastructure creates a strategic need for open-source software (OSS) and open-source hardware (OSH) for transparency.[51] Although transparency permits inspection, provable security prevents adversarial effects. Transparency also enables education, independent review, and lets non-critical infrastructure adopt these designs while making different trade-offs, e.g. to improve efficiency albeit with less security.
- The principle of eliminating complexity states that security relies on simplicity and explanation.[52] As computers and computer networks grow more complex over decades, maintenance and keeping control becomes more difficult. This 'boiling-frog' effect, where organisations slowly tolerate more glitches while pressured to deliver more and more complex functionality, pushes towards

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

> normalisation of insecure practices. Moreover, vendors drift apart, causing conceptual fragmentation and technical incompatibility. The principle states that complexity must be eliminated: the behaviour of a system must be specified as simply as possible, while the complex implementation underneath is proven correct with respect to such a behavioural specification.

One example where both principles fail is cloud migration. Inspired by C.S. Magee's "Awaiting the cyber 9/11"[53], cloud computing was proposed to make cybersecurity more manageable. While local 'clouds' aid in security and incident management, remote 'clouds' make the network in between a critical dependency beyond the control of both client and vendor. Moreover, to realise a cloud, data centre deployments use largely homogeneous hardware/software that involve large investments, which incentivise vendors to hide fundamental (hardware) security issues by creating opacity that can be mistaken for security: in reality, decades-old architectures have a large technological footprint and face decades-old critical security issues.[54] Moreover, concentrating responsibility in the hands of a few top-level experts is very risky: a single mistake can nowadays have an economic blast radius in the tens to hundreds of billions of euros, cf. the CrowdStrike incident.[55]

## Controlling the Layers of Abstraction

To grasp the complexity of cyberspace, we make use of levels of abstraction (see Figure 13.1). In the time domain, one could consider the range of operating frequencies between the petahertz (the frequency of light and cryogenic computing)[56] and the nanohertz (also called a generation, roughly corresponding to 30 years) to be at least 25 orders of magnitude. In physical space, one could consider the fine granularity of nano-scale devices,[57] each about a hundred of $(nm)^2$, all the way up to the global level near the Earth's surface at which the Internet operates, around $500T(m^2)$, to be at least 30 orders of magnitude. At each order of magnitude we recognise different components. From compositions and integrations of billions of nano-scale devices, one obtains larger components such as information processors and memory. In turn, billions of such higher-level components are linked by electrical/optical channels to create the Internet, where the number of nano-devices is approaching $10^{20}$: the most complex socio-technological system humanity ever created.[58]

Cyberspace[59] can be defined as a dynamical system, comprising the electromagnetic field and its cybernetic effects. At each level of abstraction, first-order cybernetic effects are logically explainable observations involving information flow, circularity, and feedback.[60] Recursion can explain such phenomena,[61] and

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

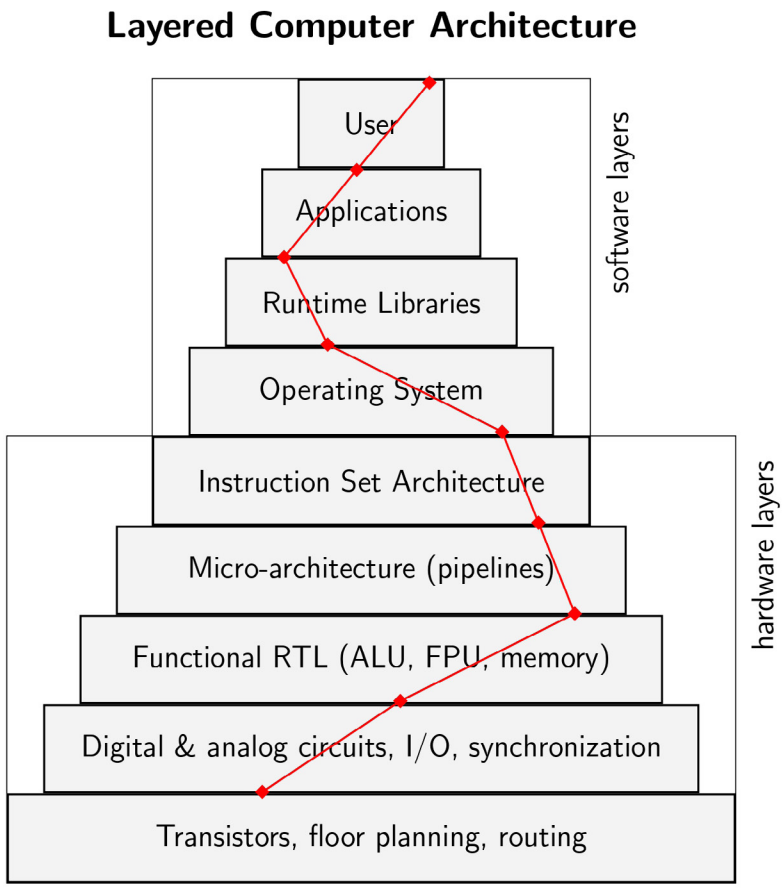



Figure 13.1: Computer architecture, both hardware and software, shown in layers. Instruction Set Architecture layer is the interface between software and hardware. The thin red line shows how flaws in different layers can be used to achieve unexpected effects in higher layers: for example, the RowHammer attack misused timing assumption at the lowest layers to cause bit flips in sensitive locations in memory to bypass defences at higher layers in the stack. It did so because under normal operation of a pipelined execution, such memory accesses would be handled by a cache (part of the micro-architecture), but the attack explicitly avoids that cache, thereby violating a timing assumption in a memory component.

mathematical logic explains relative notions of recursion and the emergence of a-causal yet synchronous effects. Second-order cybernetic effects arise when we also consider the environment, including human behaviour and physical systems, via sensors and actuators.

To raise the level of abstraction, we often ignore the intrinsic complexity of layers below, focusing only on their extrinsic simplicity: observable functionality

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

that support the layers above (Figure 13.1). Ignorance is bliss:[62] only when functionality fails do we recall the inner working of deep layers. Each level of abstraction describes desirable and undesirable functionality differently, creating communication barriers causing 'Babylonian confusion.'[63] While each layer may be correct in isolation, an integrated validation and verification approach across stacked layers is crucial for overall system quality and reliability.[64] Therefore, a common language is essential to prevent misleading abstractions.

Simple descriptions involving recursion can denote systems with complex behaviour. Handling these descriptions requires disciplined thinking as demanded by **formal methods**. Formal methods can be applied at every level of abstraction to define desirable/undesirable functionality, and to validate and verify that systems include/exclude such functionality. They are the most reliable scientific tool for ensuring, from the building blocks upward, the quality of computing and communication systems. Formal methods employ mathematics for the design and integration of systems,[65] and have a long history in high-assurance, safety-critical domains such as railway signalling, avionics, spaceflight, missile control, and nuclear power.[66] The DARPA High-Assurance Cyber Military Systems (HACMS) program has shown how to successfully apply formal methods in the military context.[67]

Zooming in on a single computer, consider modern architectures such as Intel/AMD's x86 and ARM. After the discovery of the FDIV floating point division bug, resulting in a costly product recall, Intel invested more in applying formal methods to catch errors early.[68] Deep design flaws in processors can surface years later, often uncovered through independent study, requiring active **intelligence** gathering. Recent research shows that covert side-channels in speculation-based out-of-order architectures (as used in x86 and ARM processors) lets adversaries exploit timing characteristics of caches to leak data between virtual machines sharing a physical processor.[69] When such fundamental security issues are discovered, higher-level layers should be reassessed. Hence, lower-layer design errors are costlier to fix than those above. Hardware errors are costly, especially when one considers data centre deployments, and the risk of loss of control over many areas of cyberspace, making intelligence regarding their presence highly valuable. If security risks at the theatre-level view are unknown, preparing for impact is difficult. One should not confuse the theatre-level view[70] where rare events still occur, with 'security theatres'[71] that waste resources. Intelligence on existing or potential vulnerabilities enables timely off-loading of low-quality components to less critical markets (e.g. entertainment systems), compartmentalising effects, and lowering cyber insecurity in the military context.

Adversaries penetrate systems by breaking abstraction layers in unexpected ways, generating undesirable effects at higher layers. For example, memory upscaling led to the RowHammer family of attacks,[72] exposing upper layers to new

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

vulnerabilities[73] stemming from neglect of robust software/hardware engineering standards (e.g. exhaustive time-sensitive validation and verification). These issues should be detected early in design, although they are sometimes tolerated for efficiency reasons. Interface mismatches between abstraction layers, causing assumption/guarantee violations, should be identified early via subject matter expert **surveillance**. Proper incident-reporting and pre-mortem processes are essential.[74]

New vulnerabilities and zero-day exploits in legacy systems are increasingly discovered automatically by both allies and adversaries. This activity constitutes **reconnaissance**. AI agents can scan vast networks and our complex technology stack, called the 'tower of Babel,'[75] more efficiently than most humans. While AI can aid vulnerability detection, retaining a human in the hacking loop is necessary to allow human intuition to steer the discovery process. We are not at the singularity where humans cannot keep pace:[76] nevertheless, cyber defenders should take a zero-trust approach, continuously studying unknown devices to detect emerging technologies within protected infrastructure.

Finally, Europe is considered to be lagging in independently developing computer technology. One can easily get the impression there was an implicit division of labour in NATO, where the US focused on hardware while Europe focused on software. This implicit division can partially explain Europe's talent acquisition and retention problems[77] and lack of technology transfer at universities,[78] thus remaining stuck at developing only software prototypes. As Fiott explains,[79] it is Washington's concern that Europe lags so far behind the U.S. in what is called the 'technology gap' in the "areas such as command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR)" that it may affect interoperability. Europe now has the second-mover advantage: a unique opportunity to design high-assurance computers and networks according to its own values, taking into account in system design all lessons learnt of the past decades, complying with the highest levels of common criteria for system quality.[80]

### Internet Disruptions

The Internet uses a layered architecture of protocols (Figure 13.2). A protocol is an agreement that lets computers communicate. The layers are: application (e.g. HTTP), transport (e.g. TLS, TCP), network (e.g. IPv4/IPv6, OSPF, BGP), link (e.g. Ethernet), and physical. The Internet Engineering Task Force (IETF) and the Institute of Electrical and Electronics Engineers (IEEE) publish the technical specifications for these protocols. Similar to the hardware/software split in computer architecture, network architecture is also divided into two parts:[81] IETF defines the

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

network layer and above, while IEEE defines the link layer and below. This section focuses on the most critical layer: the network layer.

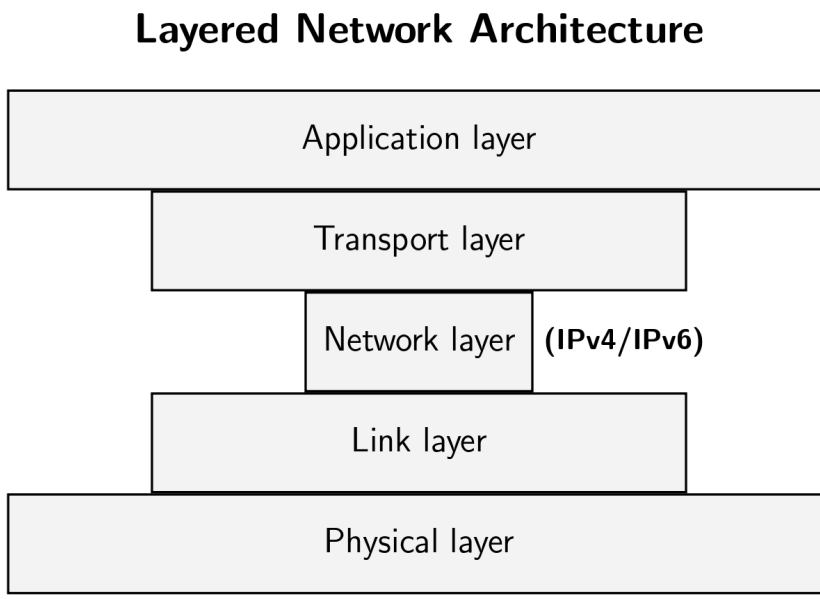



Figure 13.2: Internet networking architecture, shown in layers. The most critical layer with respect to denial and manipulation is the network layer. The figure is shaped as an hourglass due to the Hourglass Lemma.[82] The most critical layer is the network layer, where its main functionality is connectivity.

The Internet is constructed technically and organisationally. Parts of the network are grouped by an organisational entity called an Autonomous System (AS), encompassing computing devices and their communication links. They are called 'autonomous' because a single administrative entity is responsible for the devices, their security, and their interconnection also with neighbouring autonomous systems. Examples include an office, a ship, ad-hoc field networks, or a satellite constellation. Autonomous systems vary in geographic scale, some cover very wide areas.

For inter-network connections, neighbouring autonomous systems are linked by Border Routers (BRs), which are gateways between the interior and exterior of an autonomous system (Figure 13.3). Traffic entering is *ingress*; traffic leaving is *egress*. Globally, the Internet is a patchwork of ASes connected via these border routers. To reach hosts in an arbitrary AS, traffic may traverse one or more third-party ASes that provide transit, carrying traffic that does not have a host in the transit AS as a destination. These third-party ASes belong to various Internet

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

Service Provider (ISP) tiers, with the mid-tiers covering wider regions, and the top-tiers providing global coverage.

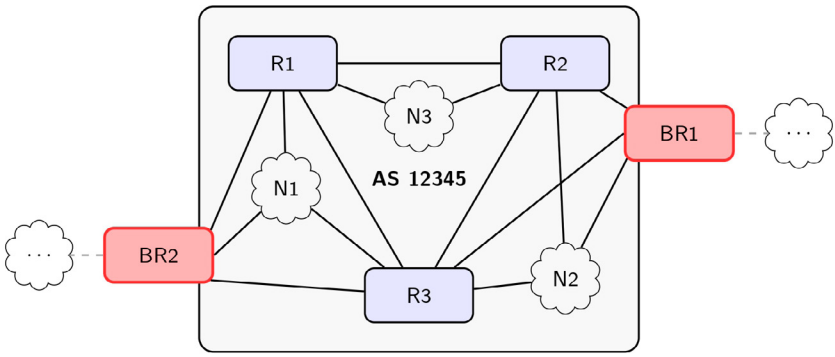



Figure 13.3: Example autonomous system, with internal routers (R1 until R3) and two border routers (BR1, BR2) connected to the outside world. Three subnets (N1 until N3) are owned by this autonomous system, so the border router publicly shares routing information regarding the reachability of these subnets, thus attracting inflow of traffic. Depending on policy, BGP can advertise that this autonomous system allows transit traffic (between BR1 and BR2): note that if the router R3 fails, there is a redundant path via R1 and R2.

The overall system supports dynamic reconfigurations: when links or routers fail, traffic flow adapts automatically. This is also required within an autonomous system, where each organisation uses different techniques for internal redundancy. Monitoring and dynamic reconfiguration tools such as Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) exist, but a global consensus on exterior traffic routing is needed: the *de facto* protocol is the external Border Gateway Protocol (BGP), which specifies route update messages and spreads route information between autonomous systems. Border routers use these update messages to direct and adjust internal traffic flows, ensuring transit traffic flows from border to border.

There are more technical details that can be found in any competent book on computer networking,[83] involving autonomous system numbering (ASN), the global IP address space (IPv4/IPv6), and the international organisations managing these, such as the Internet Assigned Numbers Authority (IANA) and the five Regional Internet Registries (RIRs). Moreover, there are many other critical issues on the Internet, involving the higher layers built on top of the network layer, such as the Domain Name System (DNS) and the Public Key Infrastructure (PKI) used for the Web. We focus on the routing system.

The Internet is not the only way to interconnect. For higher assurance, fixed lines or Multi-Protocol Label Switching (MPLS) can be used, but this requires

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

manual setup, increases reliance on single providers, and could reduce overall network resilience. Fixed lines are not shared and thus entail high costs for a single organisation. Also in the military context, recent conflicts have shown that frontline areas often depend on commodity Internet, as fixed leased lines are not always available.

Within the current organisational structure of the Internet, governing the network layer is difficult. On the BGP-controlled Internet, autonomous systems rely on an implicit notion of trust. No single party is responsible when false routing information causes disruption: the Internet is not governed by any state, nor is any state responsible for ensuring its functionality.[84] Instead, market forces and loosely managed non-profit, volunteer-driven organisations coordinate the system. This poses a risk, where market forces act contrary to the interests of local critical infrastructure providers, and thus states that rely on them.

Moreover, the market lacks incentive to improve security of high-tier Internet service providers, whose autonomous systems are high value targets while they are still trusted by many networks. Spreading false routing information from these systems, especially those employing a centralised control plane, can yield large-scale effects. The core routing protocol BGP could be turned into a 'weapon of mass disruption.'[85] The current trust model enables this behaviour: autonomous systems need not prove the intrinsic security of their control plane; trust is implicit and based solely on extrinsic observed functionality. Lacking intrinsic security, an adversary can strike a well-connected core network to demonstrate insecurity (the 'grey' areas of cyberspace). While attribution remains a difficult problem, these cyber attacks are difficult to trace back to the instigator.

Technically, the BGP-controlled Internet is also vulnerable to route hijacking, route leaking, and address spoofing by compromised or insecure autonomous systems. In a route hijacking attack, adversaries reroute traffic to ASes under their control to capture traffic. Route hijacks may seem legitimate, since many route changes are used as a mechanism to mitigate Distributed Denial of Service (DDoS) attacks. While encryption can improve confidentiality, quantum computing 'harvest now, decrypt later' attacks increase risk, and traffic metadata remains publicly visible for AI to analyse. Route leaking occurs when BGP updates accidentally or maliciously spread to unintended parts of the network, even if these updates originated legitimately. Address spoofing, a major cause of the attribution problem, injects false source and destination addresses, making it difficult to trace global traffic.

More recently discovered vulnerabilities can destabilise global routing altogether,[86] affecting availability when combined with link or router failures. Moreover, BGP was never designed to assign different trust levels to autonomous systems (e.g. NATO-country networks versus external networks). Connecting critical infrastructure and vital sectors, including military networks, to the Internet

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

expands their attack surface, causing an increase in cyber attacks. The same risk applies to the battlefield in the 'Internet of Military Things.'

More recent mechanisms to secure routing information, such as RPKI (Resource Public Key Infrastructure), BGPsec, and ASPA (Autonomous System Provider Authorisation), resulted in a system with only five centralised trust roots, one located at each Regional Internet Registry (RIR). However, controlling only a single trust root is already sufficient to undo the additional security these mechanisms intend to provide. Recent financial troubles at one of the RIRs has raised fears that its root certificate might be sold to an adversary, jeopardising the security of all RIRs. Also deployment is limited: not every part of the network is covered by these mechanisms. Hence, local connectivity is either unprotected or relies on trust roots outside of NATO. Consequently, we lack sovereign control over how the PKIs are used for routing information: a single security failure has global impact. As demonstrated in the DigiNotar breach, this risk is real.

Moreover and currently, it is technically not possible to observe and choose the paths (and thus jurisdictions) where traffic is sent over: this requirement was simply never part of the design.[87] Since Internet routing is destination-based, there is no control over how traffic should travel through different networks. Such lack of control can expose sensitive traffic to hostile or adversarial areas. More technically, BGP-controlled Internet currently offers only one 'best path' per IP address prefix. If the network dynamically reconfigures due to link or router outages, it takes time to converge to a new 'best path'. This process is relatively slow, with convergence times of up to several minutes or even hours in extreme cases, which is problematic for mission-critical applications requiring fast failover. Concurrent usage of different paths is important, especially when planning larger joint operations where one takes into account contingencies in the cyber domain, and needs to anticipate outages and congestion. Moreover, path control can be used as a mechanism to limit the attack surface of systems by tracing the path back to its origin, or (temporarily) filtering traffic based on origin.

Finally, the current architecture lacks mechanisms for ensuring hardware and software supply chain security of devices within an autonomous systems, nor is there an incident reporting mechanism that allows independent reporting of security incidents at Internet service providers – for example when the security of an IXP is breached. Critical network services need to be available locally, such as time synchronisation, root certificate authorities, certificate revocation, and domain naming. Time synchronisation ensures all subsystems share a common clock, which is essential for time-sensitive data such as short-lived certificates. Many operating systems rely on vendor-provided synchronisation services, thus implicitly requiring Internet connectivity. Prolonged outages on these services could prevent desynchronised subsystems to reconnect and recover, where

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

circular dependencies could arise: synchronisation services need valid certificates to authenticate themselves, while certificate validation itself requires prior synchronisation. Similar cyclic dependency arguments also apply to other critical services.

## A Potential Internet Crash and Reset: Practical, Policy, and Doctrinal Implications

On the current BGP-controlled Internet, trust relations between autonomous systems are unregulated, lacking transparency and accountability. A zero-trust architecture provides stronger assurance: new and unknown autonomous systems are not trusted by default, but can earn trust over time. Regular verification of trust reduces the risk of control plane compromise and thus large-scale disruptions. Non-compliance with security standards or refusal of security inspections can lead to ejection from a high-assurance network, to incentivise continual security upkeep. In anti-access/area-denial terms, 'blue' areas are proven trustworthy, 'red' zones are demonstrably untrustworthy, and the 'grey' areas contain systems whose trust has not yet been verified, or whose prior verification is now doubtful due to newly discovered fundamental vulnerabilities (see third section).

There is a growing need to connect legacy systems and infrastructures to the Internet, even when they are not IP-based or designed to be exposed to a world-wide network, due to remote-working demands and stay-at-home orders. Society's dependence on commodity Internet connectivity is increasing, and some jurisdictions now legally require governments to ensure Internet connectivity. One mitigation is to use multiple, functionally separated ISPs, but this does not protect higher-tier transit providers and Internet exchanges near the network core, where insecurities can cause cascading effects and affect traffic between nearby autonomous systems. Therefore, any improvement needs to satisfy the *local availability principle*, where connectivity has the smallest possible logical footprint,[88] meaning that, if there exists a path traversing 'blue' areas, no adversary can disrupt it. This ensures distant threats cannot negatively affect local connectivity.

In sixth-generation warfare, critical networking infrastructure and its human support are (automatically acquired) targets of cyber attacks and cognitive and psychological operations, respectively.[89] As attacks intensify, which in the 'flat Internet' has significant impact, first-order disruptions cascade and cause second-order effects. Repeated, intermittent and large-scale disruptions can cause societal collapse due to its large-scale digital dependencies, yielding a surrender to a higher power. This is what is called the 'crash' of the Internet. A well-designed system (including the Internet) must always eventually permit a reset: a return to

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

the initial state. A system satisfies the liveness property of *perpetuity* when, from every reachable state, eventually the initial state can be reached.[90] The overall system can renew and reconfigure itself before the reset completes, by adopting and deploying new technologies to prevent repeating the same kind of failure from reappearing.

The possibility of an Internet crash should be publicly known. Long ignored backbone routing vulnerabilities (colloquially known as *spina bifida*) must be fixed before resetting the system, since otherwise a reset is pointless. To preserve state sovereignty, cyberspace could be structured in a federated and decentralised manner, where each state supports its own cyber area with a domestic military-industrial base supplying high-assurance components. As each area ensures local connectivity, the federated network expands by connecting isolation domains, eventually establishing a secondary global network. Traffic can still flow between isolation domains, now with the full path of each packet known in advance, similar to air traffic control managing aircraft paths. High-assurance software and hardware, as used in avionics architectures where failures are catastrophic,[91] are also needed to protect cyberspace. The new backbone routing system remains backward compatible, to support legacy autonomous systems using IPv4/IPv6 with border routers that only support legacy BGP.

To keep global Internet connectivity stable, states could agree on international laws that prohibit intrusions into other states' protected cyber areas, treating such interference as an act of cyberwar. Each state monitors both outbound traffic to prevent it from reaching foreign protected areas, and inbound traffic to guard its own protected areas. While isolation domains still interconnect globally, due to path control the attribution problem is resolved. Within every isolation domain, essential services (synchronisation, certification, naming, and routing) remain available, and each state regulates, maintains, and verifies these critical functions. Sovereign states can (democratically) regulate their isolation domain, for example by describing basic principles to protect their enclosed humans from cognitive and psychological operations, possibly following the *U.S. Declaration for the Future of the Internet* and the *European Declaration on Digital Rights and Principles*.

This chapter ends with the following bullet points:

- NATO militaries prepare to continue their operations even during global or local Internet disruptions, underscoring Guttieri's vision of 'fighting through disruption.'[92]
- Procurement of cyber within military systems need to use high-assurance operating systems and hypervisors, that are provably secure by employing formal methods, following in the footsteps of the High-Assurance Cyber Military Systems DARPA programme.[93] This class of operating systems can already mitigate many cybersecurity issues in the very short term.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

- In the context of NATO's Crossed Swords and Locked Shields cyber exercises, future work builds a more realistic 'simulated Internet' in which vulnerabilities of the BGP-controlled Internet are demonstrated, to show the effects of 'weapons of mass disruption' in a controlled environment.
- NATO should deploy secondary 'backup' networks, functionally separated from the BGP-controlled Internet: 'galvanically isolated', separating low ground from high ground. These high-assurance networks support NATO command and control in case existing commercial Internet infrastructure is disrupted.
- All military domains support cyber intelligence gathering with additional surveillance and reconnaissance activities (C4ISR) covering their hardware/software deployments and supply chains, including critical core network infrastructure of their cyber areas. Progress should be monitored, area by area, resulting in a geographic picture of 'blue', 'grey', and 'red' cyber areas.

## Notes

1 Fitton, *Cyber Operations and Gray Zones: Challenges for NATO*.
2 Sampedro, López-Ferrández, and Hidalgo, *Digital Disintermediation*; Jyothi, *Solar Superstorms*; Birge-Lee, Apostolaki, and Rexford, *Global BGP Attacks*; Stöger et al., *BGP Vortex*.
3 Licklider, *Man-Computer Symbiosis*.
4 Reed, Van Atta, and Deitchman, *DARPA Technical Accomplishments*.
5 Roberts, *The Evolution of Packet Switching*.
6 Alberts and Hayes, *Understanding Command and Control*.
7 Andrews, *The Telephone Network of the 1960s*.
8 Shirey, *Defense Data Network Security Architecture*.
9 Livingstone, "Risk and Harm on the Internet"; Carlbring and Andersson, *Commentary: AI Psychosis Is Not a New Threat*; Wong et al., *Rising Cognitive Disability*.
10 Macit, Macit, and Güngör, *A Research on Social Media Addiction*.
11 Lungu, *War.com*; Masakowsi and Blatny, *Mitigating and Responding to Cognitive Warfare*; Kibeom, *A Study on the Concept of Cyber Cognitive Warfare*.
12 Sadoun, *PsyOp and Social Networks*.
13 Ellingsen, *Hybrid Threats as a Threat to Democracy*.
14 Krishnan, *Fifth Generation Warfare*.
15 Aytac, *Digital Domination*.
16 Schaake, *The Tech Coup*.
17 Conduit, *The Political Economy of Digital Authoritarianism*.
18 Sampedro, López-Ferrández, and Hidalgo, *Digital Disintermediation*.
19 Ciriello, Sullivan, and Mindel, *Digital Luddism*.
20 Krishnan, *Fifth Generation Warfare*.
21 Fitton, "Cyber Operations and Gray Zones"; Olmstead, *Into the Gray Zone*.
22 Krishnan, *Fifth Generation Warfare*.
23 Leenaars et al., *Next Generation Internet 2025*.
24 Sampedro, López-Ferrández, and Hidalgo, *Digital Disintermediation*.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

[25] Marengo and Tu, *Optical Theorem for Transmission Lines*; Westerveld and Urbach, *Silicon Photonics.*
[26] Loygue, Al Agha, and Pujolle, *Carbon Footprint of Cloud.*
[27] Baheti and Gill, *Cyber-Physical Systems*.
[28] Mehrali et al., *Blending Electronics with the Human Body*.
[29] Kibeom, *A Study on the Concept of Cyber Cognitive Warfare*.
[30] Reed et al., *Fractional Cyber-Neural Systems.*
[31] Raymond et al., *Key Terrain in Cyberspace*.
[32] Huston, *Hacking Away at the Internet's Security.*
[33] Caoui and Steck, *Network Diversity*.
[34] Scott-Hayward, Natarajan, and Sezer, *A Survey of Security in Software.*
[35] Guttieri, *Fighting Through Disruption*.
[36] Chuat et al., *The Complete Guide to SCION.*
[37] Russell, *Strategic A2/AD in Cyberspace*; Keithley, *Interoperability.*
[38] Krepinevich, Watts, and Work, *Meeting the Anti-Access and Area Denial Challenge.*
[39] Grant, *On the Military Geography of Cyberspace*; Grant, *Using C2 Problem Space*.
[40] Salahdine, Han, and Zhang, *5G, 6G, and Beyond*.
[41] Lallo, *Internet eXchange Points*; Böttger et al., *The Elusive Internet Flattening.*
[42] Pires, *On the Capacity.*
[43] Livermore et al., *Architecture and Control*.
[44] Raymond et al., *Key Terrain in Cyberspace*.
[45] Schuchard et al., *Losing Control of the Internet*.
[46] Grant, *Using C2 Problem Space*.
[47] Joint Chiefs of Staff, *Joint Publication 3-12 – Cyberspace Operations*.
[48] Campbell, *Generals in Cyberspace*.
[49] Alshamrani et al., *A Survey on Advanced Persistent Threats.*
[50] Bhunia et al., *Hardware Trojan Attacks*.
[51] Knoll, *Adapting Kerckhoffs's Principle*.
[52] Beach et al., *Analysis of Systems Security Engineering*.
[53] Magee, *Awaiting the Cyber 9/11*.
[54] Rushby, *Partitioning in Avionics Architectures*; Hertogh et al., *Rain: Transiently Leaking Data.*
[55] George, "When Trust Fails".
[56] Wang et al., *A Wireless Terahertz Cryogenic Interconnect*; Zota et al., *Energy-Efficient Computing*.
[57] Cao et al., *The Future Transistors*.
[58] Fuchs, *The Internet as a Self-Organizing*.
[59] Kuehl, *From Cyberspace to Cyberpower*.
[60] Heylighen and Joslyn, *Cybernetics and Second-Order Cybernetics*.
[61] Jeon, *Second-Order Recursions*; Kauffman, *Cybernetics, Reflexivity and Second-Order Science*.
[62] Kelly, *The Insider Threat to Cybersecurity*.
[63] Lipovski, *Hardware Description Languages.*
[64] Gleirscher, Foster, and Woodcock, *New Opportunities for Integrated Formal Methods*.
[65] Wupper, *Design As the Discovery*.
[66] Williams, *Formal Methods in the Development*; Rushby, *Formal Methods and the Certification*; Haxthausen, *An Introduction to Formal Methods*; Dobrovic and Lovrencic, *Application of Formal Methods*.
[67] Fisher, "HACMS".
[68] O'Leary et al., *Formally Verifying IEEE Compliance*; Gupta, Kiran Kumar, and Ghughal, *Formally Verifying Graphics FPU*.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

[69] Hertogh et al., *Rain*.
[70] Greene, *Cyberwarfare and Our Allies*.
[71] Feffer et al., *Red-Teaming for Generative AI*.
[72] Mutlu, Olgun, and Yağlıkçı, *Fundamentally Understanding and Solving Rowhammer*.
[73] Aslan et al., *A Comprehensive Review of Cyber Security Vulnerabilities*.
[74] Eisenbach, Kovner, and Lee, *Cyber Risk and the US Financial System.*
[75] Lipovski, *Hardware Description Languages.*
[76] Seewald, *A Criticism of the Technological Singularity*.
[77] Khan, *European Academic Brain Drain*.
[78] Stange et al., *Open Source Hardware in Manufacturing*.
[79] Fiott, *A Revolution Too Far?*
[80] Rushby, *Formal Methods*, 37; Bowen, *Formal Methods in Safety-Critical Standards*; Fekete, *Common Criteria for the Assessment*.
[81] Clark, *Designing an Internet*.
[82] Beck, "On the Hourglass Model".
[83] Tanenbaum, *Computernetwerken*.
[84] Shirey, *Defense Data Network Security Architecture*.
[85] Korb, *Weapons of Mass Disruption*.
[86] Sampedro, López-Ferrández, and Hidalgo, *Digital Disintermediation*; Birge-Lee, Apostolaki, and Rexford, *Global BGP Attacks*; Stöger et al., *BGP Vortex*.
[87] Clark, *Designing an Internet*.
[88] de Boer et al., *Footprint Logic for Object-Oriented Components*.
[89] Krishnan, *Fifth Generation Warfare*.
[90] Hiep, *A Reo Semantics*.
[91] Rushby, *Partitioning in Avionics Architectures*.
[92] Guttieri, *Fighting Through Disruption*.
[93] Fisher, "HACMS".

## References

Alberts, D. S., and R. E. Hayes. 2006. *Understanding Command and Control*. Assistant Secretary of Defense: C3I/Command Control Research Program.

Alshamrani, A., S. Myneni, A. Chowdhary, and D. Huang. 2019. "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities". *IEEE Communications Surveys & Tutorials* 21 (2), 1851–1877.

Andrews, F. T. 2002. "The Telephone Network of the 1960s". *IEEE Communications Magazine* 40 (7), 49–53.

Aslan, O., S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin. 2023. "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions". *MDPI Electronics* 12 (6), 1333.

Aytac, U. 2024. "Digital Domination: Social Media and Contestatory Democracy". *Political Studies* 72 (1), 6–25.

Baheti, R., and H. Gill. 2011. "Cyber-Physical Systems". *The Impact of Control Technology* 12 (1), 161–166.

Beach, P. M., L. O. Mailloux, B. T. Langhals, and R. F. Mills. 2022. "Analysis of Systems Security Engineering Design Principles for the Development of Secure and Resilient Systems". In *Handbook*

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

*of Scholarly Publications from the Air Force Institute of Technology (AFIT), Volume 1, 2000–2020*, 33–63. CRC Press.

Beck, M. 2019. "On the Hourglass Model". *CACM* 62, (7) (June), 48–57. https://doi.org/10.1145/3274770.

Bhunia, S., M. S. Hsiao, M. Banga, and S. Narasimhan. 2014. "Hardware Trojan Attacks: Threat Analysis and Countermeasures". *Proceedings of the IEEE* 102 (8), 1229–1247.

Birge-Lee, H., M. Apostolaki, and J. Rexford. 2025. "Global BGP Attacks That Evade Route Monitoring". *International Conference on Passive and Active Network Measurement*, 335–357.

Boer, F. S. de, S. de Gouw, H. A. Hiep, and J. Bian. 2022. "Footprint Logic for Object-Oriented Components". *International Conference on Formal Aspects of Component Software*, 141–160.

Böttger, T., G. Antichi, E. L. Fernandes, R. Di Lallo, M. Bruyere, S. Uhlig, and I. Castro. 2019. *The Elusive Internet Flattening: 10 Years of IXP Growth*. RIPE 78 Meeting.

Bowen, J. 1993. "Formal Methods in Safety-Critical Standards". *Proceedings 1993 Software Engineering Standards Symposium*, 168–177.

Campbell, P. 2018. "Generals in Cyberspace: Military Insights for Defending Cyberspace". *Orbis* 62 (2), 262–277.

Cao, W., H. Bu, M. Vinet, M. Cao, S. Takagi, S. Hwang, T. Ghani, and K. Banerjee. 2023. "The Future Transistors". *Nature* 620 (7974), 501–515.

Caoui, E. H., and A. Steck. 2023. *Network Diversity, Market Entry, and the Global Internet Backbone*. https://andrewsteck.github.io/uploads/SSRN-id4478868.pdf.

Carlbring, P., and G. Andersson. 2025. "Commentary: AI Psychosis Is Not a New Threat: Lessons from Media-Induced Delusions". *Internet Interventions*, 100882.

Chuat, L., M. Legner, D. Basin, D. Hausheer, S. Hitz, P. Müller, and A. Perrig. 2022. *The Complete Guide to SCION: From Design Principles to Formal Verification*. Springer.

Ciriello, R., R. Sullivan, and V. Mindel. 2025. "Digital Luddism as Collective Action to Democratise Tech". *Americas Conference on Information Systems (AMCIS 2025)*.

Clark, D. D. 2018. *Designing an Internet*. MIT Press.

Conduit, D. 2026. "The Political Economy of Digital Authoritarianism: Evidence from the Iranian Regime's Implementation of Technology". *Democratization* 33 (1), 62–84.

Dobrovic, Z., and A. Lovrencic. 2013. "Application of Formal Methods in Development of Information Systems". *Central European Conference on Information and Intelligent Systems*, Faculty of organization and informatics varazdin, 268.

Eisenbach, T. M., A. Kovner, and M. J. Lee. 2022. "Cyber Risk and the US Financial System: A Pre-Mortem Analysis". *Journal of Financial Economics* 145 (3), 802–826.

Ellingsen, T. 2024. "Hybrid Threats as a Threat to Democracy: Soft and Smart Tactics and Three Dimensions of Democracy". In *Preparing for Hybrid Threats to Security*, 36–51. Routledge.

Feffer, M., A. Sinha, W. H. Deng, Z. C. Lipton, and H. Heidari. 2024. "Red-Teaming for Generative AI: Silver Bullet or Security Theater?" *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* 7, 421–437.

Fekete, A. 2011. "Common Criteria for the Assessment of Critical Infrastructures". *International Journal of Disaster Risk Science* 2 (1), 15–24.

Fiott, D. 2017. "A Revolution Too Far? US Defence Innovation, Europe and NATO's Military-Technological Gap". *Journal of Strategic Studies* 40 (3), 417–437.

Fisher, K. 2012. "HACMS: High Assurance Cyber Military Systems". *Proceedings of the 2012 ACM Conference on High Integrity Language Technology*, 51–52.

Fitton, O. 2016. "Cyber Operations and Gray Zones: Challenges for NATO". *Connections: The Quarterly Journal* 15,109–119.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

Fuchs, C. 2005. “The Internet as a Self-Organizing Socio-Technological System”. *Cybernetics & Human Knowing* 12 (3), 37–81(45).

George, A. S. 2024. “When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 Crowdstrike Outage”. *Partners Universal Multidisciplinary Research Journal* 1 (2), 134–152.

Gleirscher, M., S. Foster, and J. Woodcock. 2019. “New Opportunities for Integrated Formal Methods”. *ACM Computing Surveys (CSUR)* 52 (6), 1–36.

Grant, T. 2015. “On the Military Geography of Cyberspace”. *Leading Issues in Cyber Warfare and Security: Cyber Warfare Security* 2, 119.

Greene, C. V. 2009. *Cyberwarfare and Our Allies: The Importance of Theater Security Cooperation*. Naval War College Newport, Rhode Island.

Gupta, A., M. V. A. Kiran Kumar, and R. Ghughal. 2014. “Formally Verifying Graphics FPU: An Intel(R) Experience”. *International Symposium on Formal Methods*, 673–687.

Guttieri, K. 2025. “Fighting Through Disruption”. *The Cyber Defense Review* 10 (1), 93–114.

Haxthausen, A. E. 2010. *An Introduction to Formal Methods for the Development of Safety-Critical Applications*. Technical University of Denmark.

Hertogh, M., D. Quakkelaar, T. Raymakers, M. H. Sarma, M. Muench, H. Bos, and van der E. Kouwe. 2026. “Rain: Transiently Leaking Data from Public Clouds Using Old Vulnerabilities”. *Symposium on Security and Privacy*.

Heylighen, F., and C. Joslyn. 2001. “Cybernetics and Second-Order Cybernetics”. *Encyclopedia of Physical Science & Technology* 4, 155–170.

Hiep, H. A. 2018. *A Reo Semantics for Reasoning about Speculative Execution*. Master’s thesis, Universiteit van Amsterdam.

Huston, G. 2011. *Hacking Away at the Internet’s Security*. https://www.dotnxdomain.net/ispcol/2011-10/hacking.pdf.

Jeon, W. 2022. “Second-Order Recursions of First-Order Cybernetics: An ‘Experimental Epistemology’”. *Open Philosophy* 5 (1), 381–395.

Joint Chiefs of Staff. 2018. *Joint Publication 3-12 – Cyberspace Operations*. U.S. Department of Defense.

Jyothi, S. A. 2021. “Solar Superstorms: Planning for an Internet Apocalypse”. *SIGCOMM’21: Proceedings of the ACM SIGCOMM 2021 Conference*, 692–704.

Kauffman, L. H. 2016. “Cybernetics, Reflexivity and Second-Order Science”. *Constructivist Foundations* 11 (3), 489–497.

Keithley, T. D. 2019. *Interoperability: The Critical Enabler in the Anti-Access Area-Denial Fight?* Marine Corps Command; Staff College.

Kelly, R. F. 2017. *The Insider Threat to Cybersecurity: How Group Process and Ignorance Affect Analyst Accuracy and Promptitude*. Naval Postgraduate School Monterey.

Khan, J. 2021. “European Academic Brain Drain: A Meta-Synthesis”. *European Journal of Education* 56 (2), 265–278.

Kibeom, K. 2025. “A Study on the Concept of Cyber Cognitive Warfare and Case Study Methodology From a Psychological Perspective”. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, 241–249.

Knoll, T. 2018. “Adapting Kerckhoffs’s Principle”. *Advanced Microkernel Operating Systems* 93.

Korb, R. A. 2025. *Weapons of Mass Disruption: How Small States Use Cyber to Resist Larger Powers*. PhD thesis, Old Dominion University.

Krepinevich, A. F., B. D. Watts, and R. O. Work. 2003. *Meeting the Anti-Access and Area Denial Challenge*. Center for Strategic; Budgetary Assessments.

Krishnan, A. 2022. “Fifth Generation Warfare, Hybrid Warfare, and Gray Zone Conflict”. *Journal of Strategic Security* 15 (4), 14–31.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

Kuehl, D. T. 2009. “From Cyberspace to Cyberpower: Defining the Problem”. *Cyberpower and National Security* 30.

Lallo, R. Di. 2018. *Internet eXchange Points: Current Challenges and New Opportunities*. PhD thesis, Università degli studi Roma Tre.

Leenaars, M., C. Valayer, C. Peyralbe, K. Billeskov, and M. Gauw. 2018. *Next Generation Internet 2025*. 30-CE-0850616/00-55. European Commission, Directorate-General of Communications Networks, Content & Technology, Publications Office of the European Union.

Licklider, J. C. R. 1960. “Man-Computer Symbiosis”. *IRE Transactions on Human Factors in Electronics* HFE, 1, 4–11.

Lipovski, G. J. 2006. “Hardware Description Languages: Voices from the Tower of Babel”. *IEEE Computer* 10 (6),14–17.

Livermore, E., R. P. Skillen, M. Beshai, and M. Wernik. 1998. “Architecture and Control of an Adaptive High Capacity Flat Network”. *IEEE Communications Magazine* 36 (5), 106–112.

Livingstone, S. 2014. “Risk and Harm on the Internet”. *Media and the Well-Being of Children and Adolescents*, 129–146.

Loygue, P., K. Al Agha, and G. Pujolle. 2025. “Carbon Footprint of Cloud, Edge, and Internet of Edges”. *Annals of Telecommunications* 80 (1), 153–169.

Lungu, A. M. 2001. *War.com: The Internet and Psychological Operations*. Naval War College Newport, Rhode Island.

Macit, H. B., G. Macit, and O. Güngör. 2018. “A Research on Social Media Addiction and Dopamine Driven Feedback”. *Journal of Mehmet Akif Ersoy University Economics and Administrative Sciences Faculty* 5 (3), 882–897.

Magee, C. S. 2012. *Awaiting the Cyber 9/11*. Master’s thesis, Command and Staff College, U.S. Marine Corps.

Marengo, E. A., and J. Tu. 2014. “Optical Theorem for Transmission Lines”. *Progress In Electromagnetics Research B* 61, 253–268.

Masakowsi, Y. R., and J. M. Blatny. 2023. *Mitigating and Responding to Cognitive Warfare*. NATO Science and Technology Organization.

Mehrali, M., S. Bagherifard, M. Akbari, A. Thakur, B. Mirani, M. Mehrali, M. Hasany, et al. 2018. “Blending Electronics with the Human Body: A Pathway Toward a Cybernetic Future”. *Advanced Science* 5 (10), 1700931.

Mutlu, O., A. Olgun, and A. G. Yağlıkçı. 2023. “Fundamentally Understanding and Solving Rowhammer”. *Proceedings of the 28th Asia and South Pacific Design Automation Conference*, 461–468.

O’Leary, J., X. Zhao, R. Gerth, and C.-J.H. Seger. 1999. “Formally Verifying IEEE Compliance of Floating-Point Hardware”. *Intel Technology Journal*.

Olmstead, M. B. 2024. *Into the Gray Zone: NATO Deterrence in a Graying and Multipolar World*. Università degli Studi di Padova.

Pires, J. J. O. 2024. “On the Capacity of Optical Backbone Networks”. *MDPI Network* 4 (1), 114–132.

Raymond, D., T. Cross, G. Conti, and M. Nowatkowski. 2014. “Key Terrain in Cyberspace: Seeking the High Ground”. *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, 287–300.

Reed, E., S. Chatterjee, G. Ramos, P. Bogdan, and S. Pequito. 2022. “Fractional Cyber-Neural Systems –A Brief Survey”. *Annual Reviews in Control* 54, 386–408.

Reed, S. G., R. H. Van Atta, and S. J. Deitchman. 1990. *DARPA Technical Accomplishments: An Historical Review of Selected DARPA Projects, Volume 1*. Institute for Defense Analyses.

Roberts, L. G. 2005. “The Evolution of Packet Switching”. *Proceedings of the IEEE* 66 (11), 1307–1313.

Rushby, J. 1993. *Formal Methods and the Certification of Critical Systems*. 37. SRI International, Computer Science Laboratory.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms

Russell, A. L. 2017. *Strategic A2/AD in Cyberspace*. Cambridge University Press.

Sadoun, A. A. 2018. *PsyOp and Social Networks*. Naval Postgraduate School Monterey.

Salahdine, F., T. Han, and N. Zhang. 2023. "5G, 6G, and Beyond: Recent Advances and Future Challenges". *Annals of Telecommunications* 78 (9), 525–549.

Sampedro, V., F. J. López-Ferrández, and P. Hidalgo. 2022. "Digital Disintermediation, Technical and National Sovereignty: The Internet Shutdown of Catalonia's 'Independence Referendum'". *European Journal of Communication* 37 (2), 127–144.

Schaake, M. 2024. *The Tech Coup: How to Save Democracy from Silicon Valley*. Princeton University Press.

Schuchard, M., A. Mohaisen, D. Foo Kune, N. Hopper, Y. Kim, and E. Y. Vasserman. 2010. "Losing Control of the Internet: Using the Data Plane to Attack the Control Plane". *Proceedings of the 17th ACM Conference on Computer and Communications Security*, 726–728.

Scott-Hayward, S., S. Natarajan, and S. Sezer. 2015. "A Survey of Security in Software Defined Networks". *IEEE Communications Surveys & Tutorials* 18 (1), 623–654.

Seewald, A. K. 2021. "A Criticism of the Technological Singularity". *The International Conference on Intelligent Systems & Networks*, 91–119.

Shirey, R. W. 1990. "Defense Data Network Security Architecture". *ACM SIGCOMM Computer Communication Review* 20 (2), 66–72.

Stange, M., N. Jäpel, D. Reichelt, and S. Ihlenfeldt. 2023. "Open Source Hardware in Manufacturing–Opportunities and Challenges". *Proceedings of the Changeable, Agile, Reconfigurable and Virtual Production Conference and the World Mass Customization & Personalization Conference*, 709–716.

Stöger, F., H. Birge-Lee, G. Giuliari, J. Subira-Nieto, and A. Perrig. 2025. "BGP Vortex: Update Message Floods Can Create Internet Instabilities". *34th USENIX Security Symposium*, 3613–3629.

Tanenbaum, A. S. 2003. *Computernetwerken*. Pearson Education.

Wang, J., I. Harris, M. Ibrahim, D. Englund, and R. Han. 2025. "A Wireless Terahertz Cryogenic Interconnect That Minimizes Heat-to-Information Transfer". *Nature Electronics*, 1–11.

Westerveld, W. J., and H. P. Urbach. 2017. *Silicon Photonics: Electromagnetic Theory*. IOP Publishing.

Williams, L. G. 1991. *Formal Methods in the Development of Safety Critical Software Systems*. Lawrence Livermore National Lab.

Wong, K.-H., C. D. Anderson, C. Peterson, E. Bouldin, L. Littig, N. Krothapalli, T. Francis, et al. 2025. "Rising Cognitive Disability as a Public Health Concern Among US Adults: Trends from the Behavioral Risk Factor Surveillance System, 2013–2023". *Neurology* 105, (8): e214226(1)–e214226(13).

Wupper, H. 2000. "Design As The Discovery Of A Mathematical Theorem What Designers Should Know About The Art Of Mathematics". *Journal of Integrated Design and Process Science* 4 (2), 1–13.

Zota, C., A. Ferraris, E. Cha, M. Prathapan, P. Mueller, and E. Leobandung. 2024. "Energy-Efficient Computing at Cryogenic Temperatures". *Nature Electronics* 7 (11), 966–974.

This content downloaded from 46.29.25.110 on Sat, 23 May 2026 08:18:44 UTC
All use subject to https://about.jstor.org/terms