MITRE | Intelligence After Next

National Intelligence Strategy Special Edition

GOAL 6

STRONGER TOGETHER: CRITICAL INFRASTRUCTURE RESILIENCE THROUGH A SHARED OPERATIONAL ENVIRONMENT

by Chris Sledjeski, Sarah Freeman, and Max Camp

© 2024 MITRE # 24-0206 1-16-2024

With the recent release of the 2023 National Intelligence Strategy (NIS), MITRE is publishing a special series of Intelligence After Next papers aligned to each of the six NIS goals the Intelligence Community will pursue over the next four years in support of U.S. national security strategies and priorities. Each paper will focus on an aspect of an NIS goal and offer a road map for success. This paper is aligned to Goal 6: Enhance Resilience

Achieving Collective Resilience

The 2023 National Intelligence Strategy emphasizes the role of the Intelligence Community (IC) in ensuring the resilience of the Nation, its allies, and its partners.[1] The strategy specifically identifies protecting the Nation's critical infrastructure through a deeper understanding of the implications of destabilizing trends and improved early warning. Transparency and robust information exchanges between the private sector and the IC will be core to realizing a state of resilience.

Traditionally, the U.S. government (USG) has leveraged public-private partnerships (PPPs) for exchanging critical information between parties. At their best, PPPs bring together multiple disciplines, authorities, and capabilities to tackle hard problems. As systems thinkers have long known,[2] all hard problems are multi-discipline. To defend U.S. critical infrastructure from adversaries' cyber operations, a PPP must bring together a diverse mix of threat vector, infrastructure domain, operations, business, and intelligence experience to understand the implications of destabilizing trends, to develop mitigation courses of action, and to improve early warning. Although sector-specific efforts have been piloted and shown progress in some sectors, they have not yet reached a scale and effectiveness commensurate to the threat across critical infrastructure.

ONLY THROUGH AN INTEGRATED SHARED OPERATIONAL ENVIRONMENT BETWEEN THE IC AND OPERATORS OF CRITICAL INFRASTRUCTURE CAN WE MATCH THE PACE OF THE THREAT ENVIRONMENT…IT IS NOT ENOUGH TO SHARE INFORMATION—WE NEED TO BE IN THE FIGHT TOGETHER.

The Office of the Director of National Intelligence (ODNI), working with relevant departments and agencies with homeland security and domestic authorities, should spearhead initiatives that address systemic issues with information sharing, transparency, and trust between the public and private sectors related to threats to critical infrastructure. This would represent a next generation PPP that leverages modern technology and enables increased data sharing, remote participation, and coordination principles. It is not enough to share information—we need to be in the fight together. That is the difference between information sharing and a shared operational environment. A shared operational environment would help industry and government realize "operational collaboration" which was a core recommendation of the 2020 U.S. Cyberspace Solarium Commission Report.

To succeed, the ODNI should promote much needed policy changes, establish standardized technical requirements, and develop capabilities to enhance the transparency and robustness of PPP information exchanges. The ODNI is uniquely positioned within the IC to advocate for and to ensure these changes are implemented.

Connections also need to be strengthened between the IC, interagency, industry, and academia, and with international organizations and partners. Only through an integrated shared operational environment between the IC and critical infrastructure operators can we match the pace of the threat environment. An integrated shared operational environment will advance analysis, improve warning, and encourage development of effective and timely mitigations that enhance our resilience at scale.

History of Critical Infrastructure Partnerships within the U.S.

The federal government has promoted PPPs as a key component of critical infrastructure protection since President Clinton issued Presidential Directive/PDD-63 on May 22, 1998.[3] Twenty-five years later, the language in PDD-63 remains relevant to discussions of critical infrastructure protection and resilience:

> *Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the government and the private sector. To succeed, this partnership must be genuine, mutual, and cooperative.*[4]

PDD-63 represents a point of origin for modern public and private partnerships, but the collaborative vision has persisted through later government initiatives and activities.

- In 2002, for example, the Department of Homeland Security (DHS) established the Protected Critical Infrastructure Information (PCII) program "to enhance information sharing between the government and private sector," and is still in use today to "analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures."[5]
- The PCII program was followed with President Bush's 2003 National Strategy to Secure Cyberspace, which also emphasized the role of PPPs in security.
- This was quickly followed by Homeland Security Directive 7: Critical Infrastructure Identification, Prioritization and Protection (HSPD-7), which directed DHS and the various Sector Specific Agencies to collaborate with the private sector for information sharing, including 1) "to identify, prioritize, and coordinate the protection of critical infrastructure and key resources" and 2) "to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices."[6]
- These concepts of cooperative security would be carried into the following administration, with President Obama emphasizing the importance of strong PPPs to ensure security, enable critical research and development, and promote cybersecurity literacy throughout the Nation.

Although sector-specific efforts have been piloted and shown progress in some sectors, they have not yet reached a scale and effectiveness commensurate to the threat across critical infrastructure. This may be due to the often-unidirectional nature of the information sharing, the siloing of information within agencies, the diffusion of data across numerous stakeholders, the inability to scale, industry concerns on how the government will use their information, and/or the lack of practical guidance for public-private cooperation among the diverse entities that must collaborate.

This shortfall also is related to the dynamics of cyber, which has shifted the operational requirements of the IC and its customers at a faster pace than any other intelligence analysis domain to date. Yet the IC continues to rely on incremental and traditional approaches in the face of a complex and accelerating digital threat. The modern threat environment for critical infrastructure, principally driven by China and Russia, includes access development, persistence, and conditions-based execution of a diverse set of destructive capabilities. In the non-kinetic space, many of these capabilities are delivered through cyber means, but the threat vectors also include supply chain, close-access, and insider means.

In the emerging threat environment, subtle anomalous events such as repeated communications or equipment failures may be the only clues that alert an infrastructure operator to the presence of malicious actors. Such an environment clearly challenges current approaches to security and the traditional intelligence cycle. Therefore, the IC should lead an evolution in PPPs.

The IC can warn infrastructure operators only about threats it can detect. In the cyber domain, adversary activity often occurs on U.S. networks launched from other U.S. networks. Restrictions on domestic intelligence collection, in turn, hamper the ability of USG entities to identify the "dots," in addition to "connecting the dots," creating an environment where USG is increasingly reliant on private sector data sources only available through robust PPPs. Again, traditional approaches will not succeed.

Persistent Challenges

Despite the IC's recognition of the importance of PPPs for critical infrastructure security, these relationships face several challenges that currently undermine their effectiveness in promoting resilience, including:

- **Unidirectionality**: Critical infrastructure operators share data with the USG but usually receive little to no actionable data in return. Additionally, a lack of feedback or transparency on how (or if) this data is used by the USG disincentivizes future collaboration. This can be particularly damaging in crisis or incident response situations, resulting in a lack of trust and inefficient crisis management. The IC also needs to manage expectations in exchanges with the private sector as to what type of information they can expect back and when and make this a more consistent experience.
- **Slow Feedback Loops**: In addition to increasing opacity, slow feedback and communication loops are insufficient to address needs in a crisis. For example, an infrastructure operator may report an anomaly to one USG entity only to have it slowly routed throughout the government. At the same time, the indicators of this anomaly expire as the adversary evolves to maintain operational security. Responses to private sector participants are further slowed by a manual, deliberative, and sometimes unsuccessful process of downgrading actionable USG intelligence and insights. Cyber intelligence, as compared with other intelligence domains, requires much faster communications as adversaries modify tools and behaviors within minutes and hours as opposed to days and weeks. It is an environment that can no longer be managed by PowerPoint slides, Word documents, and regular meeting updates.
- **Information Siloing**: Although some siloing in the IC and USG is the result of current legal requirements, it contributes to slow feedback, unidirectionality, and overall blockages in the ability of PPPs to engage in transparent and robust communications to defend critical infrastructure. Siloing has contributed to significant past intelligence failures[7] and it has been exacerbated by the introduction of an ever-growing number of Controlled but Unclassified Information handling caveats and requirements in the broader USG, which slows or prevents the IC in supporting legitimate homeland security and defense activities.[8]
- **Inability to Scale**: Because trust remains critical to the success of PPPs, these organizations are often limited and uneven in size to ensure small community dynamics and information sharing. Additionally, limited availability of higher-level security clearances and access to TS/SCI information constrain the growth of the community.
- **Lack of Practical Guidance**: PPPs lack practical implementation guidance for how participants can contribute to ensure robust, transparent information exchanges and collaboration that are repeatable and sustainable. This guidance is necessary for the shared protection of our national security, economic security, and public health and safety, and it is needed in and outside of the IC.

PPPs Currently Underway

A variety of PPPs have sought to improve information sharing and critical infrastructure resilience. Many continue to be critical, despite scaling challenges. Each has critical elements needed for a PPP and some, like the Energy Threat Analysis Center, have just recently been established. Some sectors have made progress, but no single PPP has generated the necessary transparent and robust communications needed between the IC and the private sector uniformly across critical infrastructure sectors.

- **National Cyber Forensics and Training Alliance (NCFTA)**: Established in 2002,[a] NCFTA is one of the oldest continually operational PPPs and one the Biden administration highlighted in the 2023 National Security Strategy as a standard for public-private collaboration.[9] NCFTA has operated on a pay-to-play model, with much of its support (and corresponding focus) directed to a select number of sectors, such as financial services and communications.
- **Information Sharing and Analysis Centers (ISACs)**: ISACs collect, analyze, and disseminate actionable threat information to their members and provide methods to mitigate risks and enhance resiliency.[10] They also serve as force multipliers for the dissemination of threat intelligence and concentrators for insights from their sectors. Some include government co-located, cleared critical infrastructure personnel; however, this arrangement remains difficult to scale.
- **InfraGard**: InfraGard "connects critical infrastructure owners, operators, and stakeholders with the FBI to provide education, networking, and information-sharing on security threats and risks."[11] InfraGard leverages a web portal to distribute FBI information to critical infrastructure operators. Often this model lacks feedback cycles and leaves critical infrastructure representatives in the dark about how their data is used.
- **Joint Cyber Defense Collaborative (JCDC)**: The JCDC combines government representatives, including some members of the IC, with select industry partners.[12] Traditionally the JCDC has taken a more generalized approach, focusing primarily on IT-centric adversary campaigns and non-cyber security issues (such as physical and supply chain security). Recently, the JCDC commissioned a multi-sector industrial control system (ICS)-focused collaboration initiative. It is too early to judge the effectiveness of the JCDC; however, the lack of focus on a singular sector (and associated technology) may hamper the ability of the organization to provide actionable intelligence, which has been an issue for other PPPs in the past.
- **Energy Threat Analysis Center (ETAC)**: The Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response's ETAC initiative seeks to "convene federal government and the U.S. energy sector personnel in a secure environment, joining analytic capabilities from the national laboratories with real-world threat insights."[13] The ETAC seeks to enable integration of the infrastructure, cyber, and intelligence disciplines, but as a pilot it is still working to establish the necessary USG and private sector human resources, and supporting technical tools, for real-time information sharing and collaboration. ETAC is currently is limited to the energy sector.

The State of Threat Analysis in Support to PPPs

In 2023, MITRE hosted a workshop that surveyed "Challenges in Critical Infrastructure Threat Analysis." More than 80 individuals participated from the IC, federal law enforcement, the Department of Defense, Sector Risk Management Agencies, federal interagency, and threat warning intelligence.

Participants noted that critical infrastructure threat analysis and collaboration is burdened by existing USG processes

[a] Some sources tout that NCFTA is even older and was established in 1997. For our purposes, we use the date identified on NCFTA's website.

and capabilities, which are labor and bureaucracy intensive, not always sufficiently actionable, and unable to match the pace of cyber threat activity. The workshop participants highlighted the acute need for proactive multilateral sharing of threat and infrastructure information between commercial cyber threat intelligence groups, industry operators, and the IC and USG, and for more integration.

Numerous participants stressed the need for a rapid and repeatable way that government and industry stakeholders can collaborate in an iterative way in a trusted environment. As a foreign threat-focused organization, the IC must partner to understand U.S.-based critical infrastructure operators to appreciate and assess threats. This happens but still not often enough and not in an easily repeatable and sustainable process. Furthermore, there are simply not enough infrastructure domain experts to go around in the IC—an ongoing and active partnership with infrastructure operators is essential to contextualize the implications of intelligence reporting.

A SHARED OPERATIONAL ENVIRONMENT WILL ADVANCE ANALYSIS, IMPROVE WARNING, AND ENCOURAGE DEVELOPMENT OF EFFECTIVE AND TIMELY MITIGATIONS THAT ENHANCE OUR RESILIENCE AT SCALE.

Next-Generation PPP—Defining a Shared Operational Environment

Modern defense requires collaboration and interactions at a speed and information diversity atypical for most public-private exchanges. To succeed, future PPPs should address several policy and technical issues to improve the efficacy of joint efforts to ensure the resilience of critical infrastructure. We need a much-enhanced PPP environment that includes the following attributes:

- **Enterprise-Wide Approach**: Next-generation PPPs must be capable of supporting enterprise-wide communications. This enterprise, dedicated to the resilience of critical infrastructure, needs to allow for interactions between participants from the IC, interagency, law enforcement, critical infrastructure owners/operators, national labs, and academia. The ODNI, in coordination with DHS and Sector Risk Management Agencies, should consider adopting a "whole-of-nation" approach that is more seamless than the current micro-segmentation reality that has developed sector by sector, agency by agency, network by network, issue by issue, classification by classification, and so on. This PPP must also support collaboration with international partners, as emphasized in the 2023 National Cybersecurity Strategy. Effective protection of USG information will require practical, role-based implementation guidance customized for each participant type, whether an IC member, government agency, infrastructure operator, or international partner. The IC should be a co-sponsor with the threat response, asset response, and intelligence support entities outlined in PDD-43[14] on United States Cyber Incident Coordination, as well as non-traditional interagency partners (e.g., Department of Commerce).
- **Multi-Level Classification Environment**: Any technical solution should enable multi-classification-level communications across domains. Success of next-generation PPPs will be based on a diversity of participants, many without security clearances or access to secure facilities. This underscores the need for a trusted platform and methods to authenticate contributors and the information they provide to the PPP. Any technical solution should allow for the rapid vetting, authentication, and validation of data that

b. A thin client is a basic computing device that runs services and software from a centralized server as opposed to locally managed.

is provided through PPP at various classification levels, and ensure the safety, security, and integrity of USG information. The IC should also consider how to fully extend an existing concept of "write to release" for what is now a new established customer of intelligence information beyond executive branch decisionmakers—critical infrastructure owners and operators. The ODNI should also consider how a mission area for access to critical infrastructure information could be defined to allow for a standardized level of access to streamline information sharing based on the role of government and non-government participants.

- **Virtualized Collaboration and Analytic Platform**: The technical solution will likely need to be remotely managed and maintained, potentially requiring adoption of thin clients[b] that will enable expansion of analytic tools as needed. This will allow for the USG to stand up "nimble, temporary cells, comprised of a small number of trusted operators" as needed to address emerging threats.[15] Today, the USG and IC underutilize private sector expertise and information; adoption of "virtual collaboration platforms" would enable the public and private sectors to "share information bidirectionally and work rapidly to disrupt adversaries."[16]
- **Rapid Technical Data Sharing**: The sharing of threat information cannot be a manual process. Any technology solution should leverage standardized formats, such as STIX,[c] TAXII,[d] and YARA,[e] to ensure rapid sharing of cyber technical data. However, other standardized formats are needed, such as for suspicious physical security incidents. Standardized, scalable, and machine-to-machine mechanisms will be even more important moving into the future.
- **Improved Transparency**: Opaque interactions between the government and critical infrastructure asset owners and operators disincentivize future participation. By providing transparency on how information sharing contributes to enhanced resilience, the government can overcome some perceptions of unidirectionality. Additionally, the government will need to address minor technical, but mostly policy, differences that cause or even reward siloing. These policy impediments prevent transparency and sharing and reduce the ability to scale the communications and collaboration at the speed required in a dynamic threat environment.
- **Centralized, Multi-Sector Portal**: Over the years, numerous agency-specific and sector-specific portals have evolved for the purposes of communications between industry and the government for cyber threat sharing. Cybersecurity and Infrastructure Security Agency (CISA), FBI, and others have their portals; the electricity subsector and the oil and natural subsector have theirs. Unfortunately, a side effect of these well-intentioned organic efforts is stovepiping, lack of interoperability and discoverability of data, and inefficient use of limited resources for greatest impact—no one portal has all the capabilities that each stakeholder group needs. This also leads to some sectors and agencies being underserved or unable to fully participate, which, in turn, reduces the potential resilience that would have occurred through enhanced awareness and collaboration opportunities between disciplines. Although

[c] *Structured Threat Information eXpression (STIX) is a standard based on JSON for communicating information related to cyber threats. The consistent format and terminology use reduces the burden for modeling and analysis by sharing this threat information in a well-structured format.*

[d] *Trusted Automated Exchange of Intelligence Information (TAXII) is an application protocol that enables exchanging cyber threat intelligence over HTTPS.*

[e] *Yet Another Ridiculous Acronym (YARA) is a tool that was created to assist malware researchers in their attempt to identify and classify malware samples.*

centralization presents potential concentration risks of its own, some centralization of effort is needed: a clear center of gravity for exchanges. This does not mean centralizing all data—that is not feasible due to the size and legal requirements of these vast datasets and entities. But it may mean finding ways to set up agreements for processing at the edge, at the sources, in a way akin to how DoD is starting to think about employing artificial intelligence and machine learning at the edge for joint operations.[17]

- **Homeland, Defense, and Intelligence Authorities**: To address the legal complexity of adversary cyber operations, the FBI's National Cyber Investigative Joint Task Force (NCIJTF) "leverages the collective authorities and capabilities of its members."[18] A similar approach should be employed by next-generation PPPs, because it brings together the unique powers of the IC, law enforcement, interagency, and infrastructure operators to mitigate threats. However, next-generation PPPs need a broader ecosystem than that of the NCIJTF and should be designed from the ground up to support coordination with state, local, tribal, and territorial representatives. This blended authority model is the only practical way to enable a PPP given the complexity of rules and policies that have developed around all these entities.
- **Updated Information Security Policies**: Creation of next-generation PPPs requires a change in information handling policies. These policies restrict meaningful collaboration between public and private organizations, putting lives and infrastructure at unnecessary risk. This is not to say the ends justify the means—but the current means do not serve the ends to the extent they could.

A National Imperative

ODNI should take a lead role in promoting the next-generation PPP to ensure critical infrastructure resilience and incentivize information sharing. Most information shared by this PPP will focus on cyber activity, but a next-generation PPP will need to accommodate other anticipated threats to critical infrastructure, including supply chain, close-access, and/or insider threats. This new PPP must technically enable roles for all to make better use of the collective expertise, authorities, and capabilities of this enterprise across all classification levels. Finally, it must rededicate itself to interoperability and discoverability to effectively generate a state of resilience through operational collaboration.

References

1. Avril Haines, 2023 National Intelligence Strategy, Office of the Director of National Intelligence, September 14, 2023. Available: https://www.odni.gov/files/ODNI/documents/National_Intelligence_Strategy_2023.pdf
2. Derek Cabrera and Laura Cabrera, Systems Thinking Made Simple: New Hope for Solving Wicked Problems, August 6, 2018. Independently published (June 1, 2016)
3. The White House, Presidential Decision Directive/NSC-63: Critical Infrastructure Protection, May 1998. Available: https://irp.fas.org/offdocs/pdd/pdd-63.pdf
4. Ibid.
5. Stephanie DeVos, The Google-NSA Alliance: Developing Cybersecurity Policy at Internet Speed, in Fordham Intellectual Property, Media and Entertainment Law Journal, 2010. Available: https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1280&context=iplj Fordham
6. The White House, Homeland Security Presidential Directive/HSPD–7—Critical Infrastructure Identification, Prioritization, and Protection, December 17, 2003. Available: https://www.govinfo.gov/content/pkg/PPP-2003-book2/pdf/PPP-2003-book2-doc-pg1739.pdf
7. National Commission on Terrorist Attacks on the United States, The 9/11 Commission Report: Final Report Executive Summary, July 22, 2004. Available: https://www.9-11commission.gov/report/911Report_Exec.pdf
8. Director of National Intelligence, ICD 501: Discovery and Retrieval of Information within the Intelligence Community, 2009. Available: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives
9. The White House, National Cybersecurity Strategy, 2023. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
10. National Council of ISACs, About ISACs, 2022. Available: https://www.nationalisacs.org/about-isacs
11. InfraGard, InfraGard: Connect to Protect, Federal Bureau of Investigation, February 24, 2022. Available: https://www.infragard.org/Files/InfraGard_Factsheet_2-24-2022.pdf
12. Joint Cyber Defense Collaborative. Available: https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs
13. U.S. Department of Energy, Energy Threat Analysis Center, April 2023. Available: https://www.energy.gov/ceser/energy-threat-analysis-center-0
14. The White House, PDD 43: United States Cyber Incident Coordination, July 26, 2016. Available: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
15. The White House, National Cybersecurity Strategy, 2023. Available: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf
16. Ibid.
17. James E. Cartwright and Jags Kandasamy, Employing Artificial Intelligence and the Edge Continuum for Joint Operations in Atlantic Council, 2023. Available: https://www.atlanticcouncil.org/content-series/strategic-insights-memos/employing-artificial-intelligence-for-joint-operations/
18. National Cyber Investigative Joint Task Force. Available: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force

Authors

Chris Sledjeski is a senior principal and intelligence analyst in MITRE's Cyber Infrastructure Protection Innovation Center (CIPIC). He previously served the U.S. Department of Energy's Office of Intelligence and Counterintelligence, the Defense Intelligence Agency, and the U.S. Department of Homeland Security. He continues to provide assessments on cyber threats to critical infrastructure systems for multiple U.S. government agencies.

Sarah Freeman is chief engineer for intelligence, modeling, and simulation for MITRE's CIPIC. Previously, at Idaho National Laboratory, Sarah pursued innovative threat analysis and cyber defense approaches, most recently consequence-driven cyber-informed engineering. She provides U.S. government partners and private sector entities with actionable cyber threat intelligence, developing innovative security solutions for the critical infrastructure within the United States. Her current research focus is predictive adversary analysis.

Max Camp is a capability area lead for critical infrastructure domain analysis within MITRE's CIPIC. He previously served in various staff and management roles in and outside of the U.S. federal government, covering analytic, operational, and policy advisement mission sets. Within CIPIC, he assesses and advises on threats, technologies, and security solutions for government and private sector entities.

Intelligence After Next

MITRE strives to stimulate thought, dialogue, and action for national security leaders developing the plans, policy, and programs to guide the nation. This series of original papers is focused on the issues, policies, capabilities, and concerns of the Intelligence Community's workforce as it prepares for the future. Our intent is to share our unique insights and perspectives surrounding a significant national security concern, a persistent or emerging threat, or to detail the integrated solutions and enabling technologies needed to ensure the success of the Intelligence Community. The views expressed in this publication are those of the author(s) and do not imply endorsement by the Office of the Director of National Intelligence or any other U.S. government department/agency.

Will Scannell, department manager of the strategy and policy department within MITRE's National Security Sector, is the overall manager for the IAN series. He has led development of operational concepts and implementation plans to meet changing strategic, operational, and tactical priorities and presenting strategies to inform policy deliberations at the most senior levels of the government. For questions about the series, Will can be reached at wscannell@mitre.org.

You can receive all of MITRE's Intelligence After Next papers by subscribing to the series at mitre.org/IntelligenceAfterNext

About MITRE

MITRE's mission-driven teams are dedicated to solving problems for a safer world. Through our public-private partnerships and federally funded research and development centers, we work across government and in partnership with industry to tackle challenges to the safety, stability, and well-being of our nation.

FEBRUARY 2024

MITRE

mitre.org