CYBER POLICY · NATIONAL SECURITY

The Battleground You Live In

How cyberspace became critical infrastructure, then a domain of power, and what four countries do about it.

By Scott W. Waddell, D.S.I.

LLM assistance by Claude Fable 5.1 and GPT-6 Astra.

PUBLISHED SEPTEMBER 13, 2026 • 21-MINUTE READ • PLAIN-LANGUAGE EXPLAINER

Start with the water.

In the United States, the plants that treat the water are on a list. So are the power grids and the factories, the phone networks and the banks, the hospitals and the roads. The list has sixteen sectors on it. The government calls them critical infrastructure, which is a formal way of saying that if one of them stops, people get hurt.

Here is the first strange thing about that list. Most of what is on it does not belong to the government. It belongs to private companies, and protecting it requires coordination between government and private owners.

Here is the second strange thing. The systems on that list depend on one another. Think of a bank needing power, the power company needing the phone network, and the hospital needing all three. The study at the center of this article has a word for that, interconnected, and it means that a failure in one place can spread to others.

And here is the third, which is the subject of this story. The wires are not really wires anymore. They are one network, the essential services of the country run on it, and we call it cyberspace. The United States Department of Defense counts cyberspace as an operational domain alongside land, sea, air, and space. That makes five.

The other four are familiar places of military operations. The fifth is also where you check your balance. And the study calls it something the military designation does not: a domain of power. Not the power at the wall. The other kind, the kind states hold, in a place where they compete, deter one another, and sometimes fight.

How the network became a target

It did not start this way. It started with fences.

During the Cold War, the United States worried about sabotage, and it made a list of the things a saboteur would go after: power plants, oil pipelines, defense facilities. Protecting them meant redundancy and resilience against physical attack.

The attacks of September 11, 2001 changed the list. In the years that followed, the definition of critical infrastructure grew to include the digital systems underneath the physical ones, because by then the essential services of the country had come to run on those systems. The water plant had a network. The grid had a network. The bank was a network.

In 2013 a presidential directive named the sixteen sectors and formalized information technology as one of them. The network had been promoted. It was no longer the thing that connected the infrastructure. It was the infrastructure.

Then the network kept growing. The study cites estimates that the internet's spread into a universal technology has added more than four trillion dollars to the world economy. It also cites a forecast of more than twenty billion connected devices in the coming years. Every device is also a door.

The study has a name for the idea that a country is not a pile of separate objects but a single, interlocking system. It calls it Systems Theory, and leans on it heavily. In that view, connecting critical infrastructure into one network did something more than make it efficient. It changed the nature of the risk, from isolated incidents to systemic ones that cross sectors.

The examples in the study are blunt. A breach in a financial network can disrupt global supply chains. An attack on the energy sector can cripple communications. Think of it as a row of dominoes where nobody agreed on the spacing.

The fifth domain

So the network became infrastructure. The next step was that it became a domain of power.

The study puts the shift in one sentence that is worth reading twice. Cyberspace, it says, “serves both as a battleground and as a vital enabler of economic and societal functions.” No other domain works like that. But the domain where nations now compete, and prepare to fight, is the same one where you pay your electric bill.

The United States has organized itself accordingly. Its policy rests on three pillars: deterrence, defense, and resilience. Deterrence means making an attack not worth it, by denying it success, by imposing costs, and by building norms about what states may do. The country has built offensive capabilities alongside defensive ones, and its Cyber Command sits inside the Department of Defense with what the study calls a comprehensive military cyber capability, aimed at state actors like China and Russia.

There is a live argument inside that policy. Some scholars argue that a policy of never striking first in cyberspace weakens the country’s hand. The study reports the debate and leaves it open.

And the fifth domain has a feature the others lack. It has no borders. Cyberspace lacks clear territorial boundaries, which is why states now compete to write the rules for it, and why the study says that no single country can address these threats alone. Conflict in cyberspace can reach the services people use every day.

That is why the study’s phrase fits. Cyberspace now evolves “as both a domain of power and a critical infrastructure layer.” The rest of the story is about what happens when a country has to defend both at the same time.

When the threat hit Estonia

In 2007, attacks on Estonia made these risks concrete.

Estonia’s banks and government offices came under attack. The attacks targeted the country’s digital infrastructure and threatened critical services.

Estonia's reliance on digital services left it exposed. It had built a country where people dealt with the state online, through a national digital identity system. That made it modern.

When the attacks came, the banks and the public institutions were hit together, and the people running them had to get through it together. One of the companies in that effort was Swedbank, a large private bank. The response was not the government alone. It was government and business, side by side, pooling what they had.

The study describes 2007 as the moment Estonia stopped treating cybersecurity as a technical problem and started treating it as national defense. It put cybersecurity at the front of its national agenda and rebuilt around the lesson of that year. Its neighbor Sweden took the same lesson, and began hardening its energy, finance, and telecommunications sectors as critical national infrastructure.

Today Estonia's capital, Tallinn, hosts NATO's center for cyber defense, which was established in response to the 2007 attacks. Each year that center runs an exercise that simulates a large-scale cyberattack, with private tech companies and national security forces working the same problem. Estonia keeps a backup of its most important state data outside its own borders, in what it calls a data embassy, to keep that critical data secure and accessible during an attack. Its volunteer Cyber Defence League puts private-sector specialists under a single military command when trouble comes. And when an international index ranked countries on cybersecurity, Estonia came first in Europe and third in the world.

The country that was hit became a model for others.

The next expansion

The domain is still growing, and two technologies are reshaping it.

The first is artificial intelligence. AI can watch a network and react to an attack in real time. The study calls it no longer a discrete technology but a foundational element of national security policy. But it also cites an observation that AI systems can act in ways their own creators did not expect, and they can be fooled by attackers who feed them bad data. And because AI now sits inside the defenses of energy, telecommunications, and finance, a failure in the AI can cascade through all three.

The second is what technologists call Web 3.0, a loose name for systems built on blockchains and other decentralized tools that reduce reliance on centralized control. Digital identities, contracts that execute themselves, and tokenized money are being wired into national economies. Distributed ledgers make it harder for attackers to target a single point of failure. But they also make regulation harder. Every new capability is a new dependency.

The fifth domain has one more front, and it is not made of wires at all. It is made of words. The study notes that cyber-enabled disinformation can destabilize democratic institutions and shape what the public believes. The domain where you pay your bills is also the domain where you form your opinions, and both are now contested.

The question the study asks is how a country defends a place that is at once its economy, its public square, and its battlefield, while the place keeps changing shape.

Four countries, one lens

The study is a 2025 doctoral dissertation by Scott W. Waddell, D.S.I., at the American Public University System. It asks how the United States can adapt its cyberspace policies to protect national security as AI and Web 3.0 arrive.

It looks at four countries: Estonia, Sweden, the United Kingdom, and the United States. It asks each one the same eighteen questions, three for each of six themes: how a country adapts its policies to new technology, how it handles compliance and regulation, how it gets government and business to work together, how it trains its workforce, how it protects national security, and how it cooperates with other nations.

The evidence is documents. No one was interviewed, and the study says so plainly. It rests on national strategies, laws, government reports, academic papers, and industry white papers, read and tagged passage by passage into the six themes. Add up the six theme tables and you get 989 tagged references in all.

A word of caution that the tables themselves invite. These counts tell you how often a country's documents talked about something, not how well the country did it. The United States had the most references in most tables, and one plain reason could be that the United States simply produces a great many

documents. That is this article's reading, not the study's claim. What the study does not claim is that the counts measure performance, and neither should you.

One table matters most here. In the theme the study calls national security and cyberspace resilience, the most-tagged idea across all four countries was protecting critical infrastructure. The second was cyber warfare and defense. Every one of the four countries treats both as priorities. The two halves of the fifth domain, the infrastructure and the battlefield, show up in the data exactly where the history says they should.

There is one more idea the study uses, and it answers a question that sounds too obvious to ask. If a country has good cybersecurity rules, why would it still get hacked? Because rules do nothing on their own. They need institutions to apply them, trained people to run them, and partners in business who actually cooperate.

The study's version is flat: without sustained investment in the workforce, even the best-designed policies risk becoming ineffective. Human error, it notes, remains one of the most common causes of breaches. A great fire plan is worthless if nobody in the building knows where the extinguishers are.

Three ways to defend a domain

Estonia: replace, do not patch. Estonia runs on what it calls a "no-legacy principle." When a system gets old, the country replaces it rather than layering fixes on top. That keeps the whole digital state modern and, the study argues, ready for whatever comes next.

Estonia extends its digital services to foreigners through a program called e-Residency, which lets people who have never set foot in the country register a business, bank, and file taxes under Estonian rules. It uses blockchain to protect medical records against tampering. It uses AI to detect threats and make decisions in real time. And it started early on the human side: a program called Tiger Leap pioneered computer science in Estonian schools, and its successor still helps the education ministry carry out the national cyber strategy.

Estonia's problems are just as concrete. It is small and its resources are limited, and its policy debates keep returning to the same worry: money. Scaling up a digital state takes sustained investment. It sits next to Russia, and the 2007 attacks are the reason it treats state-sponsored threats as a fact of life rather than a

hypothesis. And like every country in the study, it cannot find enough skilled people.

Sweden: the whole society. Sweden's approach is built on partnership. Its Civil Contingencies Agency, known by the initials MSB, coordinates what the Swedes call a whole-of-society approach: government, civil society, and business pulling together. A Cybersecurity Coordination Center passes threat intelligence between agencies and private firms. A Cyber Defense Act sets strict standards in sectors like finance and healthcare and requires public and private players to cooperate.

Sweden's partnerships with Telia and Ericsson, two of its telecom giants, secure the country's communications. When it built its 5G network, the government required that it be built without equipment from Mainland China. And with the rise of hybrid warfare and influence operations on its doorstep, Sweden folds cyber defense into a broader civil-military framework rather than treating it as a purely military job.

Sweden's documents contain a line the study quotes and that could stand for the whole story. "The challenge is not the technology itself, but how rapidly it changes, making it difficult for regulations to keep up." Sweden's answer to that is the same as its answer to everything: put regulators and industry leaders in a room together and keep them there.

The United Kingdom: the long game. Britain runs its cyber policy through a single body, the National Cyber Security Centre, and it plays for the long term. Its Cyber Essentials Scheme gives small and medium-sized businesses an affordable path to a baseline of security.

A threat-sharing partnership called CiSP has let government and companies trade real-time information since 2013. A program called Active Cyber Defence hands organizations tools that automatically take down phishing sites. And a program called CyberFirst reaches students from secondary school through professional training, with scholarships, internships, and apprenticeships, bringing hundreds of people with hands-on experience into the workforce each year.

Britain's worries are the mirror image of its strengths. Its own cyber agency, in the study's account, says that AI is advancing faster than the ability to regulate it. Some regions have better access to cyber education than others. And leaving the European Union meant negotiating new agreements just to keep sharing threat data with neighbors.

The country with everything

Then there is the United States, which has more of everything. It leads the world in AI innovation, and in the study's tables it leads every other case in how often its documents talk about AI's impact.

Its National Institute of Standards and Technology, NIST, built a cybersecurity framework with industry and academia that has been adopted and translated by countries around the world. NIST followed it with a framework for managing the risks of AI. The government links critical industries through Information Sharing and Analysis Centers. A program called CyberCorps pays for students' cybersecurity education in exchange for a stint in government service. And the United States runs "hunt forward" operations, working with allies to find threats before they reach American or allied networks.

So what is the problem?

The problem is that the United States is not one system. It is a federal one. Federal rules, state rules, and private-sector rules frequently diverge, and companies get caught in the gaps.

The study's example is healthcare. Federal privacy law, HIPAA, sits on top of state regulations that vary from state to state, and the mismatch delayed comprehensive security protocols and left critical areas exposed. States have their own priorities, and federal initiatives are frequently met with resistance from states that prefer local control. A company operating in several states can face several different rulebooks.

Picture an illustrative case, not a real one. A hospital chain with sites in three states has to satisfy one federal privacy law and three state cybersecurity rules, written by three legislatures with three ideas of what matters. Nothing in that picture describes any real hospital. It is simply what the study's description of the system implies.

There is a second gap, and it is about trust. Most of the infrastructure is private. The government needs companies to tell it what they are seeing. But companies worry about privacy, about liability, and about competitors, and even after Congress passed a law in 2015 to encourage sharing, many still hold back.

And there is a third pattern, softer than the other two. The study finds that the United States tends to address threats as they arise, where Britain plans ahead.

Now put that next to the fifth domain. The country that counted cyberspace as a domain, that built the offensive capability and the framework the rest of the world translates, is defending its infrastructure half with a rulebook that does not agree with itself. The study describes strong military cyber capabilities alongside fragmented civilian rules.

No country is an island

There is one theme where the four countries look most alike, and it is the one that makes the whole problem harder. Cyberattacks cross borders. All four countries belong to alliances that try to share the load.

Estonia turned the attacks of 2007 into a leadership role. It helps run the research and training at NATO's cyber center in Tallinn, and it takes part in the European Union's cyber rapid response teams, which send help across borders when a member is hit. Sweden works through the European Union and its Nordic neighbors, and it aligns its rules with the EU's data protection law, GDPR. Britain belongs to Five Eyes, the intelligence-sharing alliance with the United States, Canada, Australia, and New Zealand.

The United States takes part in the United Nations group that writes the norms for how states should behave in cyberspace. But here the American pattern shows up again in a new form. Europe has one data protection law. The United States has sector-by-sector rules and voluntary sharing, and the study finds that the mismatch complicates data sharing with allies.

An executive order that limits foreign access to sensitive American data protects the country and, at the same time, makes cooperation harder. Every one of the four faces some version of that trade-off between sovereignty and partnership.

Everyone assumes the biggest wins

The assumption has always been that the biggest economy, with the most technology and the deepest pockets, leads in cybersecurity. The study's data says something stranger.

The country with the most resources and the most AI leadership is the one whose own rules do not line up. The country that got knocked flat in 2007, with far less to spend, is the one the others are told to learn from.

The study says this directly. The analysis, in its words, challenges assumptions that larger economies inherently lead in cybersecurity innovation. Estonia's ability to innovate despite limited resources, it writes, suggests that governance agility and focused use of resources matter as much as size. It calls that a significant theoretical contribution.

Now, the catch, and it is an important one. The study does not hand the United States a blueprint. It says outright that there is no universal blueprint for cybersecurity governance, only practices that can be adapted with care. It refuses to hold up any one country as a model for all.

Its findings are a snapshot of each country at the time the documents were collected, and it warns that some of them may already be out of date. It notes that a lesson learned in a small, centralized state may not transfer to a large, decentralized one without a lot of translation. It worked from documents, not interviews, so it saw what governments said, not always what they did. And the study concedes that the author's own preconceptions could have shaped the interpretation, a risk that careful method reduces but, as the study puts it, cannot entirely eliminate.

One more honest note. Web 3.0 is in the title, but it is thin in the data. Of 184 tagged references in the policy-adaptation theme, five were about the impact of Web 3.0. Estonia, the study's digital leader, has yet to fully integrate Web 3.0 into its cybersecurity strategy.

The AI story is well documented. The blockchain story is still being written.

Who holds the domain

So go back to the list, and to the water.

In cyberspace, national defense also reaches a water plant owned by a utility, a hospital owned by a chain, a bank owned by its shareholders, and a phone in your pocket. The state can name the domain. Protecting it takes public and private effort.

That is why the study's four countries end up looking so different. Estonia put the state itself at the center and rebuilt around it. Sweden put one agency at the center and made partnership the law. Britain put one center at the center and played the long game. The United States has coordinating agencies, but its divided authority makes a shared strategy harder.

Those recommendations come down to three. First, decide who is in charge: a unified national framework, a federal task force working with CISA and NIST to bring federal and state rules into line, and a central coordinating body modeled on Britain's. Second, make partnership formal and worth it: standing

platforms where government and industry talk, real-time sharing, and tax credits, grants, and liability protection for companies that show up. Third, build the people: cybersecurity in schools from the early grades, expanded vocational training, and scholarships that create a pipeline instead of a scramble.

None of that requires the United States to become small. It requires the United States to agree on who decides.

The study ends its recommendations with a sentence a policymaker would write: "The time to act is now." That is the author's view. The author is entitled to it. The reader is entitled to a quieter one.

Cyberspace grew up as a convenience and became a place where nations compete and fight. It did not stop being a convenience when that happened. The power at the wall, the bank on your phone, the hospital across town, the water in the tap, are mostly owned by companies you have never heard of, connected in complex ways, and now sitting inside a domain of power. A country's cybersecurity is not a product it buys. It is a shape it agrees to take.

In 2007 the question for Estonia was whether it could get its banks back online. The question the fifth domain leaves for the United States is broader, because technology alone is not enough. It is not whether America has the technology. It does. It is whether America can decide who is in charge of the battleground it lives in.

Source: Waddell, Scott Wayne. 2025. Advancing U.S. Cyberspace Policies in the Age of AI and Web 3.0: A Comparative Case Study on Securing United States National Security Interests. *Doctor of Strategic Intelligence dissertation, American Public University System. ProQuest Dissertations & Theses.*

AI CONTRIBUTION STATEMENT

Claude Fable 5.1 assisted with narrative drafting and claim mapping. GPT-6 Astra performed an independent source-fidelity review.

Dr. Waddell reviewed and approved the final article and accepts responsibility for its content.

RESEARCH BEHIND THIS EXPLAINER

Move from story to source.

This explainer is drawn from the 2025 Doctor of Strategic Intelligence dissertation *Advancing U.S. Cyberspace Policies in the Age of AI and Web 3.0: A Comparative Case Study on Securing United States National Security Interests*. Explore the comparative findings interactively or consult the dissertation as the scholarly record.

RESEARCH DESIGN	SCHOLARLY RECORD
Qualitative, structured-focused comparative case study of Estonia, Sweden, the United Kingdom, and the United States using documentary evidence.	Doctoral dissertation, American Public University System, 2025. Published through ProQuest Dissertations & Theses. ISBN 979-8-3101-4740-9.

EXPLORE THE STUDY PRESENTATION →

DOWNLOAD EXPLAINER PDF ↓

READ ON PROQUEST ↗ (https://www.proquest.com/docview/3180520287)