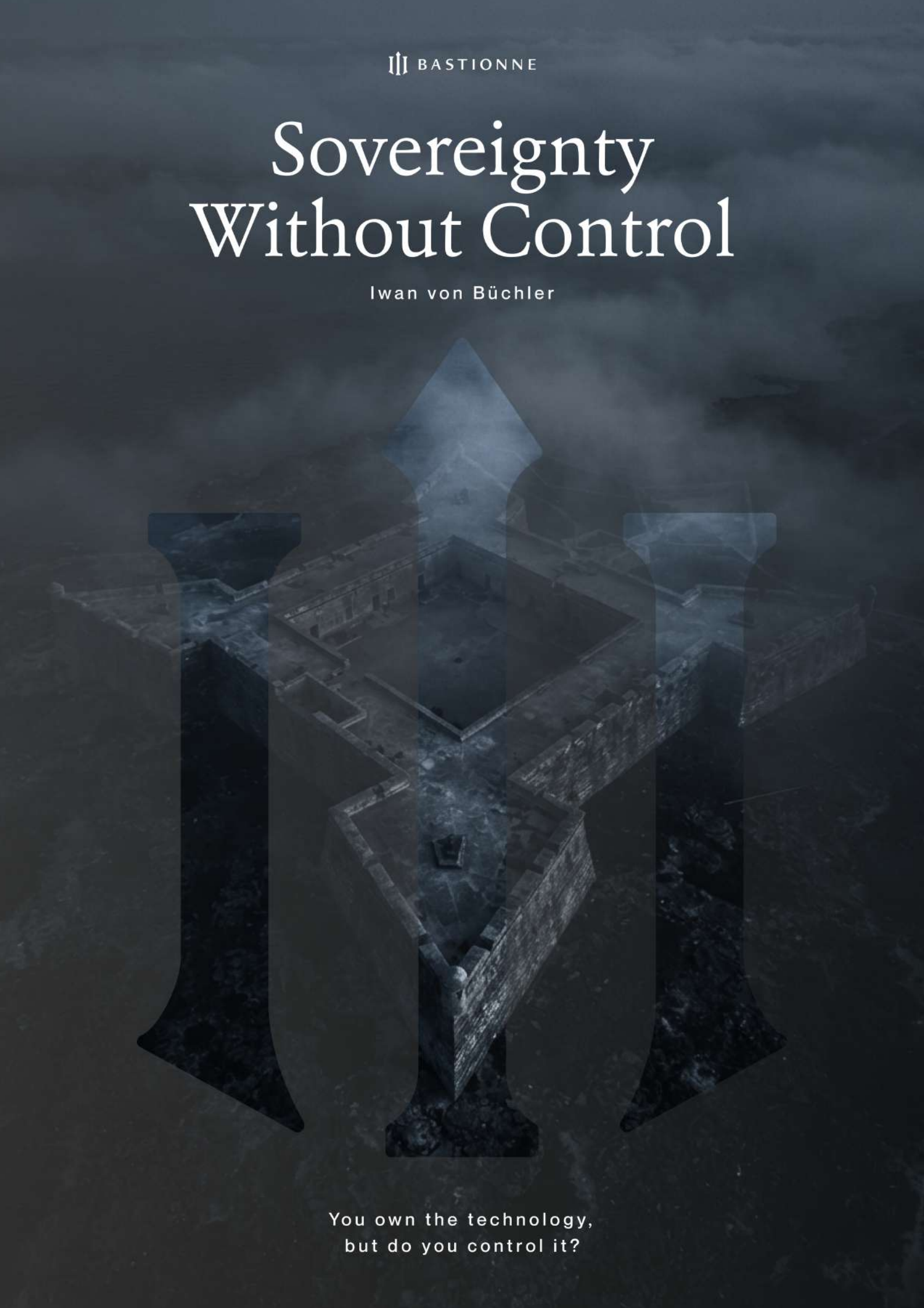
BASTIONNE

Sovereignty Without Control

Iwan von Büchler



You own the technology,
but do you control it?

Content

Abstract	3
Sovereign Control	3
How does sovereign control get denied on modern systems?	5
What does the loss of sovereign control mean for military operations?	7
How do we solve this?	8
Sovereign control in industry	9
Why does conventional cybersecurity not guarantee sovereign control?	10
Engineering sovereign control into modern systems	11
Results and Performance	12
Sovereignty without constraints	13

Abstract

Owning technology no longer means controlling it. Connected systems stay tied to manufacturers, authentication services and infrastructure that can change how they behave long after purchase.

This paper separates two ideas:

- Sovereign supply: the ability to procure, manufacture, maintain and sustain a capability.
- Sovereign control: the authority to operate that capability without outside interference or permission.

Drawing on historical cases and current military and industrial scenarios, the paper shows why domestic manufacturing and conventional cybersecurity cannot guarantee control on their own. It examines the risks posed by compromised components, software updates and trusted service providers.

It then presents Bastionne's approach: an independent control layer around existing systems. The layer governs communications at the edge, so the end user decides which connections, commands and information flows are allowed.

Technological sovereignty needs both resilient supply and independent control. Organisations should be able to adopt the best technology from anywhere and keep control of it for its whole operational life.

Sovereign Control

I write this from the heart of the Black Forest, in the historic heartland of Baden-Württemberg. As was characteristic of Germany for much of its history, this was not always part of a single unified country. The German lands were instead a complex collection of kingdoms, duchies, principalities and free cities. The Kingdom of Württemberg was no exception. And more than two hundred years ago, its rulers faced a sovereignty problem.

Napoleon was advancing across Europe and Württemberg needed the ability to arm its own soldiers. They had relied on external trade for weapons up to that point. This led to the creation of a booming arms industry here in the Black Forest, from which Mauser emerged. It is a fascinating example of a literal kingdom grasping its sovereignty with its own hands.

Sovereignty is an incredibly popular subject today. But it was equally significant two hundred years ago, and for centuries before that. It mattered then, it matters now, and it will continue to matter into the future.

What has changed is the nature of the problem. Historically, sovereignty was relatively straightforward to achieve. It might have been difficult, but the requirement itself was simple.

Consider the rifle. If Württemberg could independently procure rifles from its own industrial base, together with the ammunition and parts necessary to sustain them, it had solved its sovereignty problem. Simply because, with a mechanical system, control was implied by possession.

Once that rifle was in a soldier's hands, it was under the military's sovereign control. No vendor could remotely revoke access to it. No foreign authority could alter its behaviour. No third party could suddenly deny the soldier permission to operate it. The soldier could load it, cock it, and pull the trigger.

The historical sovereignty question therefore concerned supply: Can I obtain the rifles? Can I obtain the parts? Can I manufacture the ammunition?

Modern systems behave very differently. It is now possible for an outside party — someone other than the military operating the platform — to revoke, alter, constrain or deny control over a system even after that system has been purchased and physically placed in the operator's hands.

Possession no longer implies control. And that distinction creates a gap in the way we think about sovereignty. To demonstrate, consider the historical meaning of sovereignty. At its core, sovereignty concerns the absence of external forces capable of overriding decisions within one's own domain. Using the example of Mauser, and even the years before firearms, if a military could solve the supply aspect of sovereignty, it was sovereign.

With modern digital systems, solving the supply problem is no longer sufficient. A nation can possess a platform, manufacture parts for it, operate it with its own personnel and perhaps even build it domestically, yet an external entity can still interfere with its operation, and therefore undermine the decisions made over how that platform is used. This breaks the essence of sovereignty.

Modern sovereignty must therefore consist of two distinct requirements:

Sovereign supply: the independent ability to obtain, manufacture, maintain and sustain a capability.

Sovereign control: the independent authority to operate that capability without an external party being able to revoke, override or undermine that control.

We have spent enormous resources on the former.

The latter has been overlooked.

How does sovereign control get denied on modern systems?

A drone, for example, may seem like a closed-loop system between pilot and platform. But the drone and its controller excrete a sticky spider web of digital threads, that reaches out to ground stations, satellites and external networks. Various components rely on authentication mechanisms, APIs and network connections. Each of these connections introduce something that the mechanical rifle never had: pathways through which someone else can interfere with the pilot's control.

A compromised update, a hidden backdoor, or an unauthorised command can alter the behaviour of a system long after it has been purchased and deployed. This allows an adversary to intercept sensitive information, manipulate the data being received, interfere with commands or, in the worst case, take control of the platform itself. The system remains physically in the operator's possession. Yet the operator is no longer in control of it.

This is why many argue that we must manufacture and develop our own domestic systems. But this approach encounters a difficult reality.

Foreign supply chains are now extraordinarily difficult to escape.

Even when a drone is designed, assembled and operated domestically, its components mostly originate from manufacturers scattered across the world.

The European Parliament acknowledged this in January 2026. It found that 60% of drone components originate in the United States and China, and warned of "the dominance of certain third-country suppliers of key components such as sensors, batteries, semiconductors and rare-earth materials."[1]

1. Optics and sensors

China supplies around 80% of the global drone market, components included.[2] Most thermal lenses used in drones are produced there.[3]

These are the eyes and ears of the platform. Without them, a drone cannot reliably observe its surroundings, identify objects or perform many of the reconnaissance and targeting tasks for which it was designed.

China manufactures world-class optical components and sensors at highly competitive prices. Both matter for drones with inherently expendable lifespans.

2. Processing and electronics

Modern drones depend on semiconductors, processors, navigation chips, power transistors and other electronic components. These enable everything from flight stabilisation to image processing and communications.

Imports account for 78% of the value of chips and components used in the EU.[4] Europe's share of the global semiconductor value chain was just 9.8% in 2022.[5]

3. Battery systems

China produces more than three-quarters of the world's batteries.[6]

Batteries are fundamental to the effectiveness of modern unmanned systems. Their energy density, weight, charging performance and reliability directly influence how far a drone can travel, how long it can stay operational and what equipment it can carry.

China has become extraordinarily good at manufacturing batteries, optics and electronics at scale. Its manufacturers have invested heavily in these capabilities, and in most cases offer a competitive combination of cost, performance and availability.

This creates a grim reality. The world's most capable technologies come from the very supply chains that governments are seeking to reduce their dependence upon. And those dependencies do not disappear because the final product carries a domestic manufacturer's name.

For example, in August 2026, the British Royal Navy's Kraken K3 Scout uncrewed surface vessels were reported to carry onboard cameras that sent routine "heartbeat" traffic to China.[7]

The cameras were only components of a much larger platform. Yet they introduced an external communication pathway that could be used by adversaries to identify or locate these vessels. This does not, by itself, establish motives of espionage or malicious control.

But it demonstrates the irony:

A military can buy a domestically manufactured platform, operate it with its own soldiers and physically possess it, yet still lack control over what the platform does and who it communicates with.

Some will argue that this merely reinforces the need to manufacture not only the platform, but every component domestically.

Yet this approach introduces two further problems.

First, it is economically and industrially difficult. Recreating every specialised component, manufacturing process and supporting supply chain would require enormous resources and years of development.

Second, it can constrain capability. If an operator must reject a superior technology solely because of where it was manufactured, it may be forced to accept a platform that is more expensive, less capable or slower to deploy.

A military should not have to choose between the best available technology and sovereign control over that technology.

Alas, the problem goes deeper than foreign components.

Even a fully domestic supply chain cannot guarantee sovereign control.

Consider a drone manufactured entirely within a country's borders. The manufacturer designs the drone, writes the software that controls it, builds its cameras and sensors, and creates the electronics that make it fly. Every part of the system is developed and manufactured domestically.

What happens if that manufacturer is compromised?

What happens if its development infrastructure is infiltrated, its software signing credentials are stolen, or its employees are coerced into introducing malicious functionality?

The military physically possesses the drone. The manufacturer is entirely domestic. Yet someone else has the ability to interfere with the military's control over the drone. This is why sovereignty is no longer straightforward.

With mechanical systems, sovereign supply was sufficient to establish sovereign control. With modern systems, the manufacturer itself becomes an avenue through which control is undermined.

Sovereign control has therefore become a problem that cannot be solved by procurement policy alone.

What does the loss of sovereign control mean for military operations?

The implications are dire. Modern militaries depend on interconnected systems for reconnaissance, communications, logistics, intelligence, and tactical decisions. Consider three scenarios.

1. A compromised tactical application

Military personnel coordinate through TAK to share positions, routes, identities and operational information.

A compromised plugin, infected endpoint or unauthorised communication pathway exposes this information to an adversary. The consequences include the disclosure of operator locations, planned routes and unit identities.

The Information intended to provide situational awareness to friendly forces is instead providing intelligence to the enemy.

That information is used to prepare an ambush.

2. A weaponised unmanned ground vehicle

Take an UGV deployed ahead of a military entry team. Its purpose is to reduce the exposure of soldiers by performing reconnaissance, clearing an approach or carrying equipment into dangerous terrain.

The platform appears to function normally. But a backdoor allows an adversary to interfere with its operation.

The vehicle deviates from its intended route, abandons its task or, if equipped with weapons used to attack the personnel it was deployed to protect.

3. A compromised AI or command-and-control system

Modern command systems amalgamate information from drones, cameras, radar and soldiers on the ground, displaying it on a shared map allowing commanders to see where their forces are, where the enemy is, and what is happening on the battlefield.

A compromised component introduces false target identifications, incorrect coordinates or misleading sensor readings. The result is incorrect engagement, a compromised mission or, in the worst case, fratricide. These are three different systems. Yet they share the same fundamental failure mode. The operator's sovereign control over the system has been undermined by someone else.

Without sovereign control, the assets intended to protect you become liabilities.

How do we solve this?

We cannot simply eliminate the digital footprint of modern systems. Doing so would mean abandoning the capabilities that make these systems valuable. A drone without digital communications or sensor integration would no longer offer the same operational advantages. The same applies to new industrial machinery, tactical communications, and artificial intelligence. These technologies depend on digital connectivity.

The answer, therefore, cannot be to abandon these capabilities.

We must control them.

The digital footprint of modern systems is inevitable. The loss of sovereign control does not have to be. If sovereign supply no longer guarantees sovereign control, we must engineer around it. And once that distinction is made, an interesting possibility emerges.

An operator no longer has to choose between the best available technology and sovereign control over it.

There is a reason DJI drones have become so widely used in the private sector. The company produces highly capable drones at competitive prices, with cameras, software and flight systems refined over decades of real-world use. Rejecting such technology because of where it was manufactured may satisfy procurement policies, but it comes at the cost of reducing operational capabilities.

If an operator can independently control who communicates with a drone, what information leaves it and which commands it accepts, they can establish sovereign control over the platform, regardless of where it was manufactured. The same principle applies to domestically manufactured platforms. That said, sovereign supply remains essential.

A foreign manufacturer or government may restrict exports, withhold components, impose licensing requirements or otherwise prevent a country from sustaining its equipment. No amount of cybersecurity can manufacture a replacement battery, processor or airframe when those components are no longer available. We must therefore continue investing in domestic industrial capability. But we must recognise that sovereign supply and sovereign control address two different problems.

The former ensures that you can obtain and sustain your capabilities. The latter ensures that you retain control over how those capabilities are used. True sovereignty requires both.

Sovereign control in industry

This distinction matters beyond the military. For businesses operating critical infrastructure, factories, logistics networks and smart systems, the problem is equally relevant. Consider a manufacturer operating a fleet of connected CNC machines and industrial 3D printers. An engineer can sit in an office, send a design to a factory 200 kilometres away and have it manufactured without ever setting foot on the factory floor. Production can be coordinated across multiple locations, allowing businesses to save time, reduce costs and manufacture wherever it is most efficient.

These systems are valuable because they are technologically sophisticated. But the manufacturer must also consider what happens if their 3D printers are compromised.

Could an external party access sensitive production files?

Could machine instructions be altered?

These are questions of sovereign control. Again, this was never an issue until recent times.

A printing press from the Industrial Revolution serves as a fine example. A printer could purchase one from a manufacturer in England, install it in their workshop and operate it on their own terms. If a part broke, they could order a replacement or have one made locally. But once the press was in their hands it was under their sovereign control.

Organisations need to adopt the technology that delivers the greatest operational value. Yet the more capable and interconnected, i.e. modern, the technology becomes, the more control you surrender over them.

But a factory should not have to abandon an excellent 3D printer because it introduces unacceptable risk. And a critical infrastructure operator should not have to surrender control over its equipment to benefit from the technology inside it.

The objective should not be to eliminate modern technology. But to make it answer only to the people who own it.

Why does conventional cybersecurity not guarantee sovereign control?

This raises an obvious question. We already have encryption, authentication systems, identity management, secure communications and an enormous industry dedicated to cybersecurity. Why do these not solve the problem? The answer lies in what these technologies are designed to protect, and upon whom they ultimately depend. Encryption, for example, protects information against unauthorised disclosure and, when appropriately implemented, can protect its integrity. But an encrypted connection does not establish that the party controlling the other end is entitled to control the platform.

A perfectly encrypted channel can still carry malicious commands. Likewise, a drone manufacturer's security architecture may protect a system against outsiders while continuing to grant the manufacturer privileged access. That may be appropriate for conventional product maintenance.

But from the perspective of sovereign control, the end-user remains dependent on the manufacturer's continued integrity.

Identity and access management systems introduce a similar problem:

They establish who may access a system, by relying on identity providers, certificate authorities, authentication services and other supporting infrastructure. This introduces dependencies.

If a critical identity provider is compromised, an administrator's credentials are stolen, or a trusted signing authority is abused, an adversary is able to obtain access that the end-user never intended to grant.

The same concern applies to encryption sessions and authentication credentials, such as passwords and certificates. If an adversary obtains these keys or credentials, they gain authority over the system.

Once again, the operator's control depends on something external.

A mechanical system never had this problem. A printing press did not require a password, an authentication service, or an encrypted session to operate. Once it was in your hands, you controlled it...

But encryption itself is not the problem. Nor are passwords. The problem arises when control over a critical system depends on the integrity or availability of external infrastructure or processes that the operator cannot independently govern. In these circumstances, the mechanisms intended to protect, ironically, become pathways through which the end-user’s control is undermined.

Consider again the rifle. It would be unthinkable to place a rifle in a soldier's hands if pulling its trigger required approval from an external authentication service. Or if a vendor could revoke its operating credentials. Or if the soldier's ability to use it depended on maintaining an encrypted session with infrastructure or services outside his control.

Yet for the past 20 years, vendors have convinced us to surrender control of our systems, and called it cybersecurity.

But there is a difference between security and sovereignty:

A king who entrusts the security of his kingdom to an emperor may be protected. But he is no longer sovereign.

A system can be secure by conventional measures while leaving its operator dependent on external authority.

And this is where the distinction between cybersecurity and sovereign control becomes important. Cybersecurity is concerned with protecting systems and information against unauthorised activity.

Sovereign control asks a further question:

Who has the authority to determine what the system is permitted to do, and can that authority be undermined by anyone?

A security architecture intended to establish sovereign control must therefore consider its own dependencies. It cannot simply replace dependence on a manufacturer with dependence on a security vendor.

Otherwise, the problem has merely moved from one party to another.

Engineering sovereign control into modern systems

This is the problem we have set out to address at Bastionne. Our approach begins with a simple proposition. If modern systems can no longer be trusted to provide sovereign control by virtue of their origin or ownership, then that control must be established independently. Rather than requiring operators to replace their existing equipment, Bastionne introduces a retrofit sovereign control layer between a system and the networks, devices and services with which it communicates.

The objective is to make the end-user, rather than the manufacturer or an external service, the authority over those communications. This layer can be deployed across different types of systems, including unmanned vehicles, tactical communications, industrial equipment and other connected infrastructure.

It can operate through dedicated hardware, embedded software or virtual infrastructure, depending on the platform and its requirements. The underlying architecture is lightweight, decentralised and stateless.

Bastionne requires no external authentication services, cloud infrastructure or continuing permission from anyone. Not from the manufacturer, not from a service provider, and not even from Bastionne itself.

Instead, our technology independently verifies communications entering and leaving a protected system, directly at the edge.

External entities, including us, cannot remotely revoke the operator's credentials or withdraw permission for the equipment to operate. Once deployed, the operator has control. Anything less would reproduce the very problem we are attempting to solve.

The operator determines what is permitted to communicate with the system, and under what conditions. Commands that fall outside those rules are rejected before reaching the protected platform. Equally, communications originating from within the system are prevented from reaching unauthorised destinations.

This fundamentally changes the relationship between the operator and the manufacturer.

A manufacturer may have designed the equipment, written its software and built the infrastructure through which it ordinarily communicates. None of that grants it the authority to communicate with the equipment against the operator's wishes.

Even if a component on the platform is compromised, it cannot communicate beyond the boundaries established by the operator.

This prevents adversaries from exploiting pre-existing backdoors, allowing sovereign control to be established retroactively.

Results and Performance

In 2024, Bastionne's technology underwent adversarial testing. Across over 3.4 million attacks, no successful breach occurred.[8] This technology is now being deployed across several industries. In aviation, we are engaged with a major European airport group to enable the deployment of autonomous systems in environments where physical safety risks have curbed their adoption.

In industry, we are working with operators of connected machinery, where manufacturers retain the ability to access and interfere with equipment long after ownership has changed hands.

In defence, we are engaged with European military organisations evaluating sovereign control over unmanned platforms, tactical communications and other equipment operating in contested environments.

The equipment differs. The operating environments differ. The consequences of failure differ. But the problem is identical. Whether that equipment is a drone, an industrial machine or an autonomous vehicle. Ownership of a system means little if someone else has control over it.

This is the problem Bastionne was built to address.

Sovereignty without constraints

Two hundred years ago, the Kingdom of Württemberg sought to preserve its sovereignty by developing the industrial capacity to arm its own soldiers. The logic was straightforward. A kingdom that could manufacture its own weapons did not have to depend upon a foreign power to supply them.

And once a rifle was placed in the hands of a soldier, it was his to operate. Its manufacturer could not revoke permission to fire it, interfere with its operation from another country or demand that it remains connected to an external service.

Possession implied control. For much of history, this was a logical assumption. It is no longer true.

Today, a nation can design its own equipment, manufacture it within its own borders and place it in the hands of its own people, yet depend on external software, services and digital infrastructure beyond its control.

Even a domestically manufactured system can contain components whose operation remains subject to the authority of others. This is the distinction that we must recognise.

Sovereign supply and sovereign control are two separate requirements.

Sovereign supply concerns our ability to develop, manufacture, procure and sustain the capabilities upon which we depend.

Sovereign control concerns our authority to operate those capabilities without interference, restriction or permission from others.

We need both.

Europe must rebuild and maintain the industrial capacity to produce its own critical technologies. The ability to manufacture, repair and replace our equipment remains essential to our independence.

But that alone is no longer sufficient.

We must ensure that the technologies we possess remain under our sovereign control, regardless of who manufactured them or where their components originated.

And therein lies an opportunity.

Technological sovereignty need not mean limiting ourselves to technologies manufactured within our own borders. It need not demand that we abandon foreign innovation, duplicate every industrial capability or accept inferior equipment simply because it was produced domestically.

We should develop our own industries and strengthen our own technological capabilities. But we should also retain the freedom to procure and deploy the best technologies the world has to offer. Without surrendering control of them.

A European military should be able to operate foreign-manufactured unmanned systems without giving their manufacturers the ability to interfere with a mission.

An industrial operator should be able to purchase advanced machinery without accepting external access to its factory.

And a nation should be able to adopt technologies from anywhere in the world without placing its critical infrastructure at the mercy of those who supplied them.

These are not contradictory ambitions.

This distinction lies at the intersection of history, industry, defence, and the changing nature of political authority. It is a subject dear to me, and the reason we are building Bastionne. Our objective is not to determine which technologies others should use, but to ensure that the decision remains theirs. Not merely when the equipment is purchased, but throughout its operational life.

For centuries, possession and control were linear concepts. The digital age broke that relationship. Possession no longer implies control.

It is time to restore it.

1. European Parliament, *Drones and new systems of warfare – the EU's need to adapt to be fit for today's security challenges*, 2025/2088(INI), adopted 22 January 2026.
2. Royal United Services Institute (RUSI), *Drones: Decoupling Supply Chains from China*, November 2025, citing M. Kroenig and I. Bayoumi, *A Global Strategy to Secure UAS Supply Chains*, Atlantic Council, June 2024.
3. RUSI, ibid. (industry interviews).
4. Polish Economic Institute (PIE), September 2026, reported by PAP.
5. European Court of Auditors, Special Report 12/2025, *Microchips: EU off the pace in a global race*, citing a European Commission forecast (July 2024).
6. International Energy Agency, *The battery industry has entered a new phase*, March 2025.
7. *The Telegraph*, 9 August 2026.
8. Measured during Project Sagan, an open adversarial environment with unrestricted attack attempts and techniques, results observed during the exercise and contributed to winning the 2024 InnCyber Innovation Award.