# Governments need private-sector firepower to fight the next cyber war

Governments cannot defend national digital infrastructure alone as AI accelerates attacks, cybercrime becomes industrialised and private companies control much of the technology on which states depend, warns **Steve Durbin**, Chief Executive of the Information Security Forum (ISF)

Cybersecurity is a contest between attackers and defenders. For far too long, governments have been defending their turf alone while attackers frequently target public-sector entities with little to no resistance, launching attacks with national ramifications. Despite rules and regulations meant to establish baseline controls, attacks continue to define a growing threat landscape.

The harsh reality is that the threat surface has grown wildly beyond what governments can realistically defend.

The digital infrastructure that governments aim to secure is a product of private companies. There are limits to what the state can secure on its own, which means the focus must shift to closer collaboration with the private sector.

Let's take a closer look at why an ideal defensive and offensive posture for risk management should entail a more collaborative effort from the government.

### 1.Rise in the scale and complexity of cyberthreats

Modern cyberattacks have gone many notches higher in terms of cadence, scale, and sophistication. Such attacks do not depend on a single vector. Palo Alto Networks found that 87 per cent of intrusions across more than 750 incident response cases targeted multiple attack surfaces, from endpoints and networks to cloud infrastructure, SaaS, apps, and identity. Intrusions spread laterally across connected systems, so defending one layer well isn't enough when attackers can pivot through multiple access points in the same campaign.

### 2.Growing attack surface underpinned by everyday dependencies

Years ago, the attack surface felt like an attack on the organisation's operational perimeter. Today's attacks have moved beyond this perimeter to include the functional elements of any organisation, including cloud platforms, APIs, vendors and managed services providers. These third-party dependencies broaden the attack surface, giving cyber attackers more avenues to exploit. A compromise of a remote support tool enabled attackers to access multiple U.S. Treasury Department offices, an example of how third-party access can become the easiest entry point.

### 3.Technology ownership controlled by private entities

There was a time when major technology shifts and advancements were a direct outcome of research funded by different government entities. Examples of that include the origins of the internet, global positioning systems (GPS), solar energy and many others. But things have changed, and it is the private sector that now drives technological advancements. Critical digital infrastructure is overwhelmingly built and operated by private entities, and the government doesn't have total control over all its operational levers. This demands a change in thinking, requiring them to partner with the private sector to secure the infrastructure on which a country depends.

### 4.Cybercrime has gone industrial and is very persistent

Cybercrime is an industry with different specialisations, services, tooling and repeatable playbooks. And this industry is decentralised, meaning arresting one group doesn't dent the scale and scope of attacks in general; there is always another group to fill the gap. This is because the underlying incentives remain strong. As a case in point, crypto scams and fraud pulled in roughly US$17billion last year, fuelled by a sharp rise in impersonation schemes (up 1,400 per cent year-on-year). In November a ransomware attack on OnSolve CodeRED forced the emergency-notification platform offline, disrupting alerts used by law enforcement and other public agencies.

Considering cybercrime is the gift that keeps on giving, a coordinated response targeting the entire criminal enterprise model, including its hosting services, identity abuse, laundering pathways and scam infrastructure, is the only way forward. Get aggressive offensively, rather than continuing to play whack-a-mole.

### 5.Geopolitics enters the fray as nation-states use cybercrime

State-enabled cybercrime has become routine and normalised as an instrument of espionage, influence and strategic disruption. State-sponsored operators not only showcase greater capabilities but also a deeper reach, traversing global platforms, third-party infrastructure, and cross-border supply chains. Organisations are already on high alert, with 64 per cent accounting for geopolitically motivated cyberattacks in their risk mitigation strategies.

'National cyber defence' cannot be purely national in execution. It has to include alliance coordination and cross-border collaboration with private-sector operators that manage key visibility and control points.

### 6.The accelerating role of AI as an attack enabler and defender

AI is cutting cyberattack timelines by as much as 100-fold. Intrusions that used to unfold over days now play out in minutes. In one-in-five cases, data is already leaving the environment within the first hour. Organisations are rushing AI systems into production, adding new models, plugins, connectors, and data paths, which widens the attack surface further. Legacy controls weren't built for that pace or that sprawl. This is why governments can't solve it alone. The workable path must involve better public–private coordination, where threat intelligence disseminates faster, secure AI patterns are built and shared, and governance is aligned across sectors.

The road ahead is more about building a shared defence paradigm that moves at adversarial speed. Governments can still set the standards of accountability, but improved resilience will only come from stronger public-private coordination, faster inter-agency sharing, secure-by-design-AI, and joint disruption of criminal infrastructure across borders. ■

### Further information

To find out more about the ISF's work on cyber security and information risk management, visit **www.securityforum.org**.

**ABOUT THE AUTHOR**
Steve Durbin is Chief Executive of the Information Security Forum (ISF), an independent association dedicated to investigating, clarifying, and resolving key issues in information security and risk management by developing best-practice methodologies, processes, and solutions that meet the business needs of its members. ISF membership comprises the Fortune 500 and Forbes 2000.