European Repository of Cyber Incidents

// Comment by J. A. Lewis

Should the EU and its Member States strengthen active cyber defence measures?

History offers imperfect precedents to explain the current international situation, but it is in the context of this situation where we must consider whether Europe should strengthen its active cyber defence. One precedent comes from the 1930s, in which indecisive and unprepared democracies were inexorably dragged into war. Another is from the 1960s, in which the prospect of nuclear war led opposing sides to build a framework of agreements and understandings that provided stability and reduced the chance of warfare.

Whether our experience will be like the 1930s or the 1960s remains to be seen, but our choices now will shape outcomes later. Active cyber defence is one such choice. While cybersecurity has improved, it remains inadequate and deterrence is threadbare. A simple count of the steadily increasing number of hostile incidents is evidence of this. Weak cybersecurity encourages opponents to continue their malicious acts unabated.

The unspoken question is whether active cyber defence is merely a polite way of saying offensive cyber operations. While in reality, it is not, a policy for active cyber defence must nevertheless include the full range of response measures, including interfering with adversarial networks to collect information and potentially take disruptive actions. It may be best to think of active cyber defence as a series of graduated responses to exert pressure on those who have rejected a rules-based order.

The strategic environment for European defence exists in the shadow of nuclear weapons. Since Russia became a nuclear power, followed in short order by several other countries, nuclear armed states have avoided major wars with each other.

About the Author

J. A. Lewis is Senior Vice President, Pritzker Chair, and Director of the Strategies Technologies Program at the Center for Strategic and International Studies. He delivered this comment during his Transatlantic Keynote at the EuRepoC Conference 2024.

18 June 2024 German Institute for International and Security Affairs (SWP)

The fearsomeness of nuclear weapons restrains actions against other nuclear powers, but not against non-nuclear states. The constraining effect of nuclear weapons on warfare remains a subject of debate, but one reason states like Iran pursue nuclear weapons is that they believe that it protects them from invasion and attack; the experiences of Iraq and Ukraine suggest Iran may have a point.

Nuclear powers, however, are not constrained in using cyberattacks against non-nuclear states or in using cyberattacks against any state if these attacks stay below an implicit use of-force threshold. Espionage, crime, and political manipulation flourish in this environment. Our opponents are aggressive, inventive, and well-resourced, and they see no reason to stop their activities. While deterrence is frequently invoked in discussions of cybersecurity, it is often misunderstood. Cold War deterrence was predicated on demonstrated capabilities and opponents' belief in a willingness of a state to use these capabilities, all embedded in a process of negotiation. These conditions do not exist today in the cyber realm.

This creates an awkwardness for European security. Only France has nuclear weapons. The European Union itself is not a nuclear power and the departure of the UK from the EU dealt a grievous blow to European nuclear, intelligence, and cyber capabilities. Only a few European nations have adequate cyber capabilities; most lack them, and other than NATO, Europe does not have a coordinating mechanism for military and intelligence activities.

Creating a Defence Commissioner will not change this. Member States guard their prerogatives jealously and security in the traditional sense has been outside the remit or "competence" of the EU. An adequate defence requires capabilities that Europe is not currently capable of providing, whether due to structure or resources. It requires investment not only in weapons and munitions, but in space and cyber assets. A technical intelligence architecture is expensive. The US and China have made these investments, and Russia has its tattered Soviet legacy, but the EU faces a long and costly road.

NATO, although a defensive alliance, has made real progress in defining its role in cybersecurity; furthermore, its members include the US and the UK, countries that are nuclear powers and that have advanced cyber capabilities. However, NATO's role in a more assertive cyber defence may be limited as countries prefer ad hoc coalitions using legal and economic tools rather than military means.

For cybersecurity, the immediate problem is to foster accountability. Accountability has always been difficult for the international community. A framework for accountability exists, but it is usually ignored. The UN Charter, international law, state practice, and the norms agreed in the 2021 OEWG define responsible state behaviour, but there are no consequences for transgressions.

Active cyber defence uses the traditional levers of international relations to counter transgression. The elements of active cyber defence are attribution, a menu of proportional responses, a framework for collective action, and the political will to act. It is also essential, as part of a larger European and alliance strategy, to find ways to engage seriously with opponents who resist serious discussions.

Agreement on anything is a distant prospect, as no nation is willing to make concessions and, unlike with nuclear weapons, cyber does not pose the existential threat that could compel negotiations. However, negotiations are key to building stability, and active cyber defence may help bring opponents to the table. The alternatives are unappealing.

The rationale for active cyber defence is to create accountability by imposing consequences and changing the incentives that shape opponent behaviour. Consequences can create accountability. While consequence is a somewhat fraught term in diplomatic circles, accountability for malicious cyber actions is essential. If nothing else, a failure to act only encourages opponents.

Active cyber defence has two objectives. The first is to create disincentives for malicious cyber actions. The second is to create incentives to negotiate. It has been a decade since the last serious cyber talks. If Russia and China observed the norms of state behaviour and cooperated in cybersecurity, risk in cyberspace would largely vanish. Cybercrime would continue, but it would be manageable and not pose strategic risk. At the moment, Russia, China, Iran, and North Korea have no incentives to reduce attacks or to negotiate.

The first step in active defence is the ability to attribute the source of malicious acts. Attribution explains actions to the international community and can compel political leaders to act. This is not the attribution required in court, but rather information sufficient to persuade political leaders that a response to a malicious cyber action is justified. Deciding how to act upon this evidence is a political decision.

This political attribution has different evidentiary standards than those used by courts. An overly legalistic approach cedes advantage to opponents, and it is essential to recognise that political attribution involves assessing the culpability of a state, not an individual. While “false flag” operations are frequent, misattribution is rare in sustained engagements in which the same actors operate for years. Attribution is difficult, but not impossible, and the difficulty of attribution should not be an excuse for inaction.

Attribution is itself insufficient for defence – naming and shaming sounds nice but is utterly ineffective. After attribution occurs, states must consider appropriate consequences. Devising ways in which states can impose consequences will be necessary to increase accountability and improve the overall security environment.

Consequences entail the range of internationally lawful responses available to states that are victims of malicious cyber actions. Consequences must reflect state practice on the use of diplomacy, coercion, and force, tailored to the gravity of the incident and the nature of the offender. The work of the Counter Ransomware Initiative points to a nascent collective approach for attribution and accountability.

The development of a menu of such measures, consistent with international law, can build consensus among nations on how to respond. This menu need not be limited to offensive cyber operations, though these should not be ruled out. Active cyber defence can include offensive cyber capabilities, but these are only one tool among many.

Offensive cyber capabilities involve the ability to penetrate the networks of another state to collect information and, perhaps, to engage in disruption. Only a few European countries have such cyber capabilities. Even the US, which has advanced cyber capabilities, has been reluctant to use them, despite what one may read about active defence and “defend forward.”

This reluctance is understandable. The central concern that explains this reluctance is a fear of escalation. Our opponents, particularly Russia, use the fear of escalation as a method of manipulation and constrainment, but there has never been an incident of escalation in the long history of cyber conflict. This suggests the fear is overstated and that escalation risk from active cyber defence can be managed as part of a larger European strategy of engagement and defence.

The consequences most likely to arise in active cyber defence will be countermeasures or retaliatory acts using legal and diplomatic tools such as sanctions or indictments. Consequences must be both proportional to the initial incident and consistent with international law. Sanctions are appealing, but targeted sanctions on individuals or agencies appear only to annoy adversaries and are insufficient to change their behaviour. The question is whether there is political support for broader sanctions more likely to change adversarial behaviour.

Imposing broad sanctions is politically challenging, so responses must consider scale, proportionality, duration, the costs of cyber sanctions, and whether a response is to individual action or a larger campaign. It is important to recognise that adversarial states' actions, while they may be detected sporadically, are often part of larger, sustained campaigns. This suggests there is a major analytical problem for European (and transatlantic) strategy, as our opponents may have a harsher view of the contest and are less risk averse.

Finally, active cyber defence is most effective if it is built upon mechanisms for collective action among like-minded states. This can be on a voluntary basis – states are not ready for binding agreements on consequences – and can implement aspects of existing measures, such as the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities or the Counter-Ransomware Initiative.

While there has been some progress in imposing consequences, such as sanctions by the EU or indictments and sanctions by the United States, it has been an ad hoc and episodic process that has not increased the observation of norms nor stability in cyberspace. A collective response to a cyber opponent might change this. It may be politically more palatable to say that active defence builds deterrence as it creates credible threats of repercussions that persuade opponents to change their behaviour.

It is important that states agree to respond collectively to malicious cyber actions; consistent action by a group to impose consequences for malicious cyber actions is essential to creating accountability. Action requires a public commitment at senior political levels, years of high-level engagement, and a constant reiteration towards adversaries of the need for responsible state behaviour. One of the most important steps that can be taken to improve cybersecurity is to make such actions routine within the diplomatic agenda vis-à-vis states like China, rather than simply sporadic objections.

Active cyber defence challenges an already complex effort to build up collective European security. Europe's defence architecture must balance the roles of the EU, NATO, and the United States. Europe will need to determine how best to structure cybersecurity partnerships with NATO and the United States within a difficult security environment. Europe must decide how much it can rely on alliances and how far it wishes to pursue (and pay for) sovereign defence.

Attribution, consequences, and collective action can set us on the path for accountability that goes beyond cyberspace. The benefits may not be immediately observable, but the old approach to cybersecurity of simply hardening network defences and sharing information is inadequate. There are risks in using active defence, but these risks are smaller than those if we continue on our current course. There is reluctance to acknowledge that the time when conflict could be avoided is over, but what is clear is that the next step is to build on the Cyber Diplomacy Toolbox and use partnerships with NATO and the United States to foster active cyber defence.

Much of what we do now in cybersecurity is to describe and gawk at the problem. The current strategic approach to cybersecurity puts democracies in a reactive position. Change will not come without a greater acceptance of risk and the actions needed to manage it.