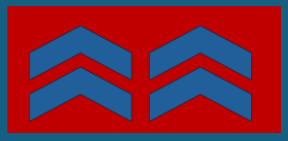
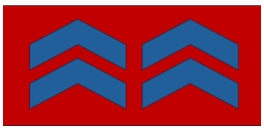
Legislative and governance international frameworks for Artificial Intelligence in the area of national security
- Position Paper Series -

Diana Popa



RED SKY 4

www.redsky4.nl



Popa, *Diana (2025). Legislative and governance international frameworks for artificial intelligence in the area of national security. Position Paper Series.* Red Sky 4, 2025.

Legislative and governance international frameworks for artificial intelligence in the area of national security. Position Paper Series

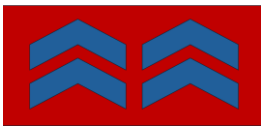
By Diana Popa

June 2025

The rapid development of artificial intelligence has surpassed the speed with which regulation can be formulated and legislation passed for its regulation. This is the case in most countries and technology development maintains its distance advantage in relation to accompanying regulation and legislation. Admittingly, innovating and regulating at the same pace is by no means an easy task and aiming for synchronized international alignment brings additional challenges. Lead countries in the field of AI feel the pressure even mode acutely, given the speed of technological development in the AI field. Top level view from such contexts leads to question such as ”Do we allow ambition to outpace responsibility? Or do we rise to the challenge to innovate and to regulate, to lead and to safeguard?” (Dutch Minister of Defence at the 2025 Shangri-La Dialogue), indicating assumed positioning towards how technology is developed and regulated.

Legislative and governance frameworks for mainstream AI

In the case of mainstream AI deployment, similar challenges equally faced by technology deployers and regulators in their respective countries have led to initiatives aiming at harmonisation frameworks and initiatives for developing overarching international governance frameworks. There are national or regional characteristics of technology regulation, with some states or regions (such as the EU) being inclined to horizontal, general approaches to regulating technology and others more prone to preferring and encouraging sectorial level approaches. The high-level, general approaches need to be broad enough in order to allow for interpretation and application, while at the same time not requiring periodical action by the legislator, thus potentially allowing for more room for applications that can be contested afterwards. The sector level approach brings development and application of the regulations closer to the specific

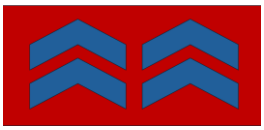


needs of the sector and potentially can allow for an easier overcoming of differences in national level approaches.

Adding to the potential for discrepancies between countries or regions are different approaches regarding the priority relation between technology development and technology regulation, with some regions prioritizing market self-regulation and competition driven technology development - the US- (or what one might call ambition) others opting for comprehensive regulatory action - the EU, others developing government driven technological development and deployment – China, and others embracing a symbiotic approach, stimulating societal adoption of technology and regulating at a slower pace in response to and in tune with the pace of adoption, such as Japan.

Efforts for consolidation of AI international regulatory frameworks indicate the attention given to harmonization efforts, likely needed in the case of cross-border deployment and international markets. While the practicality of these exercises serves the efforts of regulators, either from the public sector or corporate, the dedication of time and resources towards these efforts is a matter of choice, and again reflects a certain approach to technology development and preference or priorities (for the market – the US; legislation – the EU; government control - China). Examples of attempts of global or international AI governance frameworks include initiatives such as the G7 initiated Hiroshima AI process, the AI Statement initiated at the 2025 Paris AI summit or the REAIM initiative on responsible AI in the military domain. Adherence to these initiatives remains very much a matter of choice, with signatories deciding to join according to adjacent interests and potential for conflict with other priorities. Regulatory actions remain very much in the realm of nation states. Even in "federated" systems such as the EU, where regulations receive direct application in national legislation, regulatory action can change in response to technological advancement and more importantly in response to political shifts. Admittingly, this can be a slower process, but not an impossible one. Ultimately the legislative system is a reflection of the political state at a certain point in time, applied synchronically and interpreted as such diachronically.

An additional inflection point can manifest itself after political change. In the case of AI regulation, the 2025 change in the national US administration also brought the revocation of the previous administration's regulation over AI. Changes of legislation are influenced by how power mandates are attributed between the different branches of government and the culture of a given environment, oriented either towards slow, stable or predictable system change or quite the opposite, having the potential for radical change due to accumulation of powers or inclination towards innovation through disruption. Moreover, both recent and historical events indicate that with changes in the political system or administration, political driven purges in key areas of interest such as national security are not a rarity, even though publicly motivated,



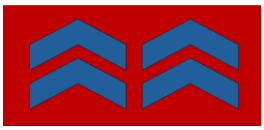
for reasons of damage or image control, as a necessity for resizing of over bloated national security structures. Yet, despite adjustments in terms of occupancy, the system should be robust enough to assure continuation and mandate fulfillment.

There are thus areas that remain under the exclusive mandate of the state. Sovereignty in the cyber and intelligence areas is still veery much a national matter and despite calls for overarching or international structures, they should and most likely will continue to be so. AI development and implementation is part of national security strategies (for example the UK 2025 National Security Strategy focusing on developing national AI capabilities) in terms of capacity development and simultaneous corresponding risk mapping, formally indicating the potential this frontier technology has in the national security field.

Potential for international AI frameworks in the National Security area

In comparison to mainstream applications, regulation and legislation over AI use in the national security space is far more difficult to develop in an international approach, if possible or desirable at all, as further argued here. Efforts to establish new mechanism and structures to bridge these traditional exclusive realms are driven by necessity (rising threats or war) but very often meet with practical or systemic resistance from the practitioners. Deployment of AI within critical infrastructure and other objectives of interest for national security is conditioned by technological development at national level, technology path dependent choices and influenced by assumed objectives and means to reach them. As such, discrepancy is expected in relation to the technological choices and TRL's found in different states.

When it comes to how technology is regulated and which stakeholders are consulted in the process, inquiries into the potential conflict of values are part of regular debates in Western society. In the case of technology deployment for mainstream AI, these become positive stimulants for self-clarification and potentially implementation of best solutions.



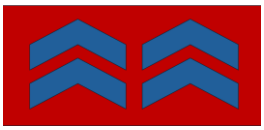
In the case of higher level decisions, questions regarding conflicts of values become more prone to either revealing system weakness or diluting decision making capabilities due to focus on second order effects. Thus, in a very territorial field in terms of practices and customs, under the mandate of national states, such as is the case of the national security area, attempts to harmonize practices and regulatory actions remain limited by the necessity of solving concrete challenges and potentially opening dialogue for mutually beneficial exchanges of solutions.

In the intelligence field, nations decide how much they want to share and both collaboration and competition can be subject specific. Calls for new international cooperation mechanisms embedded within existing structures such as the EU and NATO might find support from policymakers, but still remain limited by national mandates. As I made the case elsewhere (Popa, 2025) often a multiplication of centralised structures results in mere policy multiplication, with little or slow impact or change on effectively reaching the assumed objectives. Further more, liaison work is in practice influenced by political decision making, and on the ground collaboration can be interrupted given top-down decision making.

Thus, given the practical challenges brought forward by the technology itself, the territoriality of the legislation and that of interests and practices, international harmonisation efforts lack in both practicality and most likely desirability, in terms of regulatory action or soft law and even more so in terms of legislative initiatives or hard law. With the area of national security inherently bound by aspects of secrecy, regulatory action becomes restrictive in terms of court competency and even more so due to the intersectionality with technological aspects that are not fully of easily explainable.

It is anticipable that in the national security area as well, visible and widespread deployment of technology can faster receive a form of consensus, given practical incentives and requirements to do so. At national level, internal conflicts can be solved through legislative harmonisation actions and cumulation of jurisprudence. Tensions regarding assumed responsibility on a potential controversial high impact deployment can be solved procedurally by means of presidential orders or government level supervisory committees, depending on the legislative system itself.

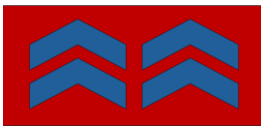
In an international context however, the initial dialogue sparked by the wish to tackle common challenges might lead to the conclusion that practice and legislative harmonization is undesired (taking the example the EU, where harmonization is conducted across multiple areas while others, such as national security, remain in the mandate of the national governments). Once dialogue is initiated and case studies deployed and analysed, incompatibilities and fault lines can become visible. In addition to the formal system of legislation, western societies observe value incursive introspection from different streams of society in regards to limits on means



and methods used for national security purposes. Questions such as "How far can you go in a democracy with the mandate of intelligence or national security", testing democratic resilience when under pressure by means of focusing on ethical frameworks can become a self-brake in adopting international frameworks regarding technology adaptations. Internal system cohesion in terms of legislation, regulation or espoused values would have to face increased tension points when meeting different systems of political and social organisation and most likely would lead to attesting to core incompatibilities of approaches. As such, previous results of these harmonisation exercises showing lack of consensus should not come as a surprise. Moreover, these introspective and harmonisation exercises might lead to opening a Pandora's box if accountability of AI deployment becomes a test for the robustness of the legislative systems itself. This can be a destabilising factor, having at times intended push external factors, for testing both resilience of the engaged parties and abiding by prior agreements.

The deployment of technology in this semi-legal or grey space is not necessarily to be understood as being against the law, but it can be a result of legislative void. On the other side, creating new legislative frameworks might also not be practical, since context specific deployment might be characterised by singularity. Additionally, regulatory actions in the mainstream areas of technology have shown that overregulating can have a limiting or restrictive effect. Doing so in the area of national security can prove to become counter-productive, being the opposite of a mandate enabler. The international law system to this day has numerous grey areas in terms of applicability and potential for interpretation and even more so in territory bound aspects or contested spaces.

While international harmonisation efforts in the area of AI regulation have been abundant, recent government changes in the West have shown that the West is no longer one conglomerate, internally attuned with universal democratic values. The stretching of the democratic values spectrum raises questions regarding the necessity and desirability of further engaging in international harmonization efforts, considering that the distance between the extremities of the category implies adjustments that could be either less attuned with self interest or ephemeral in effect. Adding to this the different views or cultures towards the drivers of technology, makes the international harmonization process that more challenging. One should also consider that attempting to extrapolate harmonisation exercises outside the theoretical democracy spectrum would prove having even less chances of success.

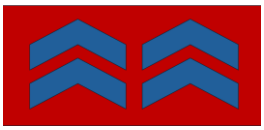


As mentioned in the example regarding changes in state administration, politics does influence both how AI is regulated and how it is embedded in practice and law within different branches of activity. A potential international agreement is more likely in areas where stakes are at their highest and reciprocal attention as well, such as in the case of AI embedded in nuclear capabilities, or in the case of main stream, low impact applications where alignment has some practical benefits. In the case of AI used for defensive purposes, accountability is balanced against often existential or grave threats, thus making value alignment a question to be ex-ante rationalised and responses calibrated to different risk levels.

With different publics in democratic regimes having to be convinced of supporting certain high impact decisions or with the public questioning post-factum the means or measures of state power when perception of infringement of liberties takes shape, democratic principles can become counter productive, especially in a resource scarce environment. While autocracies consume time and resources for maintaining control over the narrative, democracies need to allocate time and resources to assure a win between competing narratives and order of priorities. The matter of convincing the public becomes even more arduous when faced with explaining choices that have an economical impact on the general public, even in matters such as national security or defence. This is even more the case given the credibility of the threat towards the national interest, or perception of its imminence, is influenced at the population level by the distance to it, which often translates in aspects regarding visibility. Governments having to convince the general population and specific sectors on the need to allocate a higher percentage of the budget to defence purposes (including national security in the same or different expense category) at the expense of other sectors, thus also have to convince the public of the imperative necessity of doing so.

This distance from the threat, and existing technological capabilities and legislative context will influence the manner of deployment of disruptive technologies in the national security sector, again leading to discrepancies in capabilities and objectives. Yet another reason for any overarching harmonisation frameworks to remain an expressed desiderium motivated by diplomatic reasons or at manifested at the higher levels principles.

The modular character of AI, meaning the possibility to be embedded in different platforms, thus enhancing the potential of the respective technological base or process, makes the aspect of governance frameworks and risk management particularly challenging when it comes to AI. This is easily exemplified in the case of AI enhanced drones. In the case of drone deployment on the battlefield, “mounting” multiple AI modules on a drone increases its efficiency in terms of goals (for example increasing success rate of strikes in the case of targeting systems, or



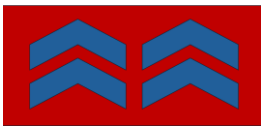
increasing situational awareness). The combination of different AI modules in a technological platform can increase the efficiency of the platform exponentially and systemically. It also brings additional challenges that often only post-factum can be rationalised and systematized in regulatory frameworks. The possibility of remote deployment and deployment across jurisdictions complicates the matter of regulatory actions and their limits even further. Another accessible example comes from the case of wartime deployment of AI enabled drones, where pilots are removed from the battle ground and can even be located in different countries, without actually having been to the target location, making issues of combat engagement complex in matters of status of active combat of the pilot and in broader terms diffusion of responsibility. From a military institutional perspective, cumulating reports of emotional disengagement of drone pilots also raises concerns regarding training and ex-ante preparation and post-factum support for such virtual combat missions.

Defence organisations are therefore internally looking into the use of algorithms within existing ethical and juridical frameworks. This parallel internal and external inquiry, in addition to being a lengthy and time consuming process, leads to results which most often take the form of policies which again, remain at the discretion of the sovereign states to adopt or not. Within defence alliances, AI policies can be adopted by the units of the organisation themselves, but the adoption of any policy developed at alliance level remains at the discretion of the sovereign states to implement within their own structure and procedures. This leads to partial results and indicates towards the inefficiency of attempts for coordination in the defence and national security space.

External factors influencing chances of international alignment

With increasing threat levels, increasing and reaching technological and digital sovereignty has long been on the agenda of governments and their agencies responsible for the protection of the physical and digital space. Recent defence strategy documents and policy papers have taken a starker tone towards the imperative of achieving this sovereignty as soon as possible, given increased threat levels, while at the same time underlining existing competition in the technological field and the importance of having asymmetric advantages.

The latest national security strategy of the UK (2025) seems to indicate towards assuming the position of a fortress consolidating its walls and being ready to close its gates, while projecting forward facing deterrence: “[...] trends in the national security [...] include: confrontation with adversaries (indirect and potentially direct); competition with other states (which will be both

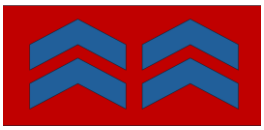


systematic and strategic in nature); and cooperation (which will become harder but arguably even more important than ever before)" (UK's 2025 NSS:16)

It seems thus logical that in the competition for technological supremacy, even between allies, all parties would first weigh the impact of giving away strategic advantages through the potential of disclosure in dialogues or initiatives for developing international frameworks. Expressed objectives of increasing lethality of national defence capabilities and those of military alliances, and increasing risks of leeks with the dissemination of information further indicate to the need and incentives for capabilities stealth. Protecting first-adopter advantage becomes a stimulant for protection of exclusivity even between allies. Thus, the often lamented speed of regulation not being able to keep up with technological advancement can become an advantage for rapid innovation stimulation in a space of legislative void that servs strategic objectives. In a highly competitive world, securing and maintaining access and exclusivity of disruptive technologies will be a strategy that will have quantifiable practical benefits, though for reasons of alliance maintenance not presented as such.

Given difference in technology innovation profiles at national levels, different clusters of technological innovation speed or maturity emerge. Technologically advanced states will look to engage with others of at least similar capabilities if not higher. Should international frameworks prove beneficial, countries found leading in the competition for technological advancement will want to be part of the ones setting the rules. We therefore witness the formation of strategic alliances in the competition for technological supremacy, with clusters being named in national and collective security strategies not according to geographical proximity but according to similar levels of technological maturity and interest alignment. Protection of crown jewels in terms of technological development becomes a matter of national priority and international cooperation on the matter is incentivised after the conditions for protecting the first have been meet and by perceived mutually beneficial and long term factors. In parallel, these transactional alliances can also lead to "regulatory blocks", as the UK's 2025 NSS suggests, since international alignment might be a facilitator for increasing competitiveness.

Additional relevant points for the case here are found in the UK's '25 NSS: 1. complete sovereignty is not possible in fields such as AI and quantum, meaning that 2. "some technologies will need to be accessed via reciprocal agreements and partnerships with like-minded partners" and 3. wanting to enter these reciprocal agreements of "ivy league" technology developers will mean having a high level of technology development. This becomes



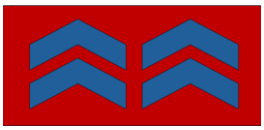
an additional stimulant for innovation and selectivity in terms of alliance forming, based on different arguments, as presented above.

Another point to consider is that in some countries such as the UK, the types of actors present in the technology side of the national security area have multiplied, raising questions as to the applicability of legislative streams, division of responsibilities between developers of technical solutions for national security and national security agencies actually deploying the solutions. The multiplication of actors and type of actors sees also a blur in categories, with companies of different sizes and types emerging. A similar debate regarding defence responsibilities takes place around the blurred division of responsibilities for the protection of cross-border critical infrastructure found under private or corporate portfolio.

Previous attempts at reaching international agreements with optional character being agreed upon only by some participants indicate again that this is just what they are – signs of benevolence for finding solutions in the limits of self-interest or diplomatic efforts, at best. This is also a reflection of a time not as tense as the one we are observing at present. As such, with the assuming of this more or less obfuscated internal and external competition in a context of concrete external threats that become mutable in terms of targets of manifestations, reaching international agreements on value sensitive issues that are deeply connected to national interests seems a reminiscence of times gone by.

An adjacent disruptive trend is noted. With the West not being one monolith anymore, through the shift towards a more transactional style of interaction on the world stage, old alliances are being accompanied or replaced by transactional alliances between states that not so long ago seemed to have incompatible systems of values or were adversaries in the economical, geopolitical and technological fields. Indication towards this trend is found also in the ’25 UK NSS: “it may become more common to work more closely with those with different values where mutual interests are identified. Agility and flexibility will be crucial” (UK’s 2025 NSS:18) underlying the idea of a shift towards transnationalism and “pragmatic bilateral deals and mini-lateral groupings”. Arguably, in a more adversarial world, alliances allowing for communication channels to remain open offer the pretext for engaging in interactions that can give insights into competitive or even adversarial camps.

Thus, in this more transactional world, “across the spectrum alliances” become less often the case and also most likely downscale, becoming subject based and interest mutual. This strategy however can present inherent conflicts. An exemplification of this is the current case in the Indo-Pacific, where considering the shift in the security landscape, from the Western perspective it was considered undesirable that countries in the region partner with China in the economic sector and with the US for defence purposes, given conflicting interests between the



two actors in one area. This would *de facto* limit or direct the choice of the country towards one pole of power or another.

The question remains, in this new context of multi fronts conflicts, with common external threats and in the same time internal competition, what place do international frameworks still have?

Popa, Diana (2025). ***Legislative and governance international frameworks for artificial intelligence in the area of national security. Position Paper Series*****. Red Sky 4.**

About the author.

Diana Popa has over 17 years of experience in research and academia and has authored numerous reports and scientific articles. Recent research and analysis focus on resilience as part of defence programmes, emerging disruptive technologies, in particular Artificial Intelligence in high risk areas, including national security and defence.

Red Sky 4
The Netherlands
www.redsky4.nl
Redsky4@ziggo.nl