Artificial Intelligence/Machine Learning and Cyber Command as a Tool of War: A New Method in the Mediterranean Battlefield?

Firas Sassi
Senior Director of National Security and Geo-Strategy
The Institute for Prospective and Advanced Strategic and Security Studies (IPASSS), Gammarth

> "We're at the beginning of a golden age of AI. Recent advancements have already led to invention that previously lived in the realm of science fiction – and we've only scratched the surface of what's possible" – *Jeff Bezos*

When are we going to establish a full-domain cyber dome for the Mediterranean region? When are we shifting our strategy from reacting after-the-fact to anticipating an event and pre-empting incidents?
In 2012, a group of Iranian-backed hackers launched the biggest ever DDoS attack on 46 financial sector firms in the United States and Europe. In December 2015, Russian military intelligence services conducted a destructive cyber attack against the Ukrainian power grid that left most of the country in darkness. In 2020, a satellite-controlled Artificial Intelligence (AI) rifle assassinated a nuclear scientist and the infamous STUXNET virus compromised centrifuges in a nuclear plant. And there are countless other notable examples in the public domain.
I envision a cooperative effort of like-minded allies creating a cyber dome for the Mediterranean. A multi-country and multi-agency cyber/AI dome structured around a C6ISR system (Command, Control, Communications, Computers, Cyber-defence and Combat Systems, Intelligence, Surveillance and Reconnaissance).
Our world's major battles are fought in silence and secrecy, between soldiers thousands of miles apart and on computer screens. Cyberwarfare is devastating, highly refined, relatively inexpensive and a distinctly effective method of harming one's enemies.

To enter into this arena responsibly, we have to address the following checks and balances. How can we ensure mutual-capacity building? How would we manage escalation, proliferation, and ensure government continuity after a major AI-based cyber attack? What are the rules of engagement in cyberwarfare? How do we report emergent risks and respond to incidents?
Have we considered the ethical and legal implications of such questions? Are laws and regulations relevant to today's readily available tools and methods? How do we perfectly balance privacy with national security? Where can we deploy AI/cyber defence/cyber offence technologies as a tool of war?

Artificial Intelligence/Machine Learning

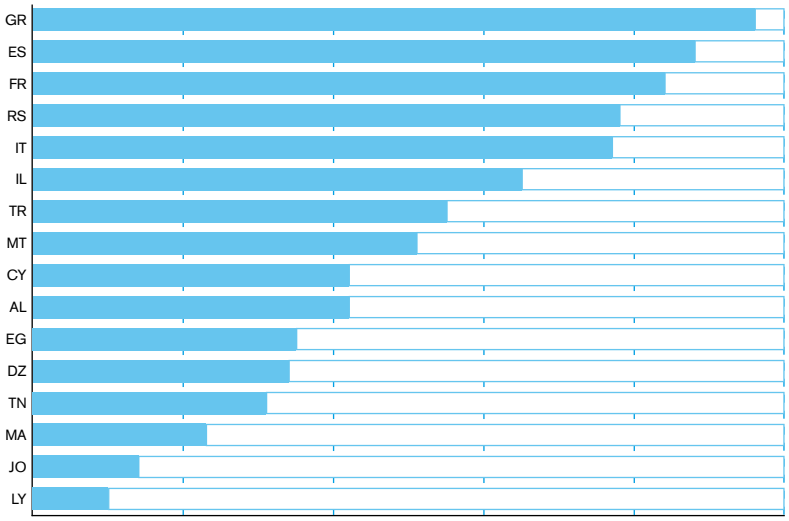
Artificial Intelligence/Machine Learning (AI/ML) systems can now learn, identify, select, understand, analyse, surmise, deduce and even anticipate. Advanced data processing capabilities offer the promise of digesting large volumes of information, thereby helping military decision makers choose the most effective courses of action.
Addressing these challenges will require Mediterranean cooperation between government and industry. Mediterranean and North African allies bound by common values and a shared interest in promoting the digital economy can work together against a common enemy.

Cybersecurity

> "Cyber attacks as a strategic matter do not differ fundamentally from older tools of espionage and sabotage" – Noah Feldman

CHART 15 **The National Cyber Security Index (legislation in force)**

Rank	Country	National Cyber Security Index
1.	Greece	96.10
5.	Spain	88.31
9.	France	84.42
17.	Serbia	77.92
19.	Italy	76.62
30.	Israel	64.94
51.	Turkey	54.55
58.	Malta	50.65
73.	Albania	41.56
74.	Cyprus	41.56
81.	Egypt	35.06
86.	Algeria	33.77
96.	Tunisia	31.17
105.	Morocco	23.38
127.	Jordan	14.29
140.	Libya	10.39



Source: www.ncsi.ega.ee May 2021.

Cyber criminals come with varying degrees of sophistication, backing and resources. They can be organized crime groups, lone hackers, hacktivist groups and nation state attackers.

Nation state attackers are arguably the most dangerous because they are not driven by emotion or zeal like a terrorist. They are deliberate, calculated, well funded and supported with the resources to target anything they deem worthwhile.

Cyber attacks can take the form of phishing attacks, password attacks, man-in-the-middle attacks, Distributed denial-of-service (DdoS) attacks, SQL injections, remote access tools, eavesdropping, ransomware or hacking data for espionage purposes.

Mediterranean Capability

In the Mediterranean, cyber capabilities are unequally distributed, with France, Spain, Greece, Italy and Israel leading the race. Cyber-commands and cyber-military units are growing in number and great progress is being made in cybersecurity using AI.

North-South Actors and Tools

France, Spain, Greece and Italy are taking big steps to make their cyberspace as secure as possible. Various NATO initiatives or the Tallinn manual considers "cyberspace" as a full domain in the battlefield. The other states in the South are trying to catch up with the paradigm shift. While advancements in regulatory and national strategy are being made, their cyberspace remains extremely vulnerable.

Our world's major battles are fought in silence and secrecy, between soldiers thousands of miles apart and on computer screens. Cyberwarfare is devastating, highly refined, relatively inexpensive and a distinctly effective method of harming one's enemies

Med North-South Comparison

The e-Governance Academy's NCSI offers up-to-date public information on how prepared states are for preventing cyber threats – it is a capacity-building index. If we compare statistics (in the graphics

CHART 16 **Cyber Incidents Response Capacity**

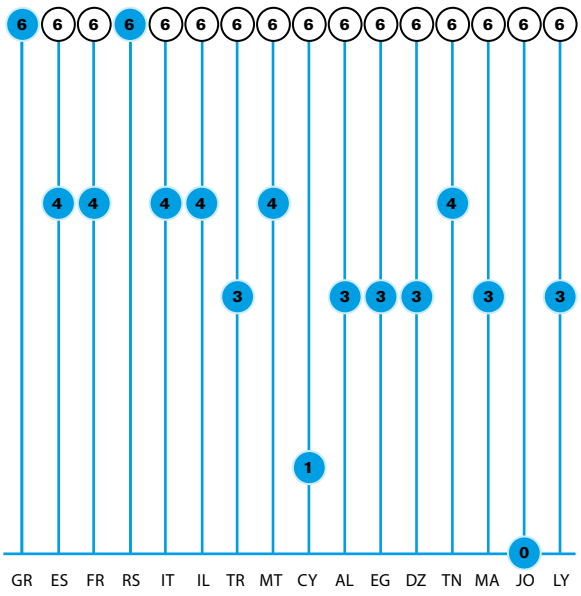


CHART 17 **Military Cyber Operations May 2021**

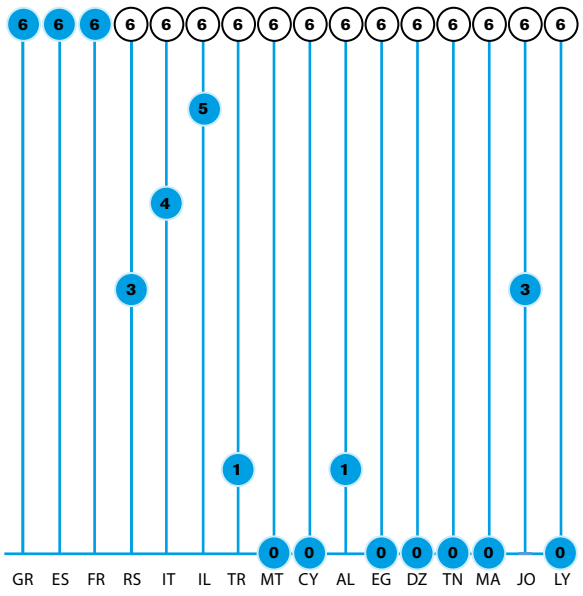
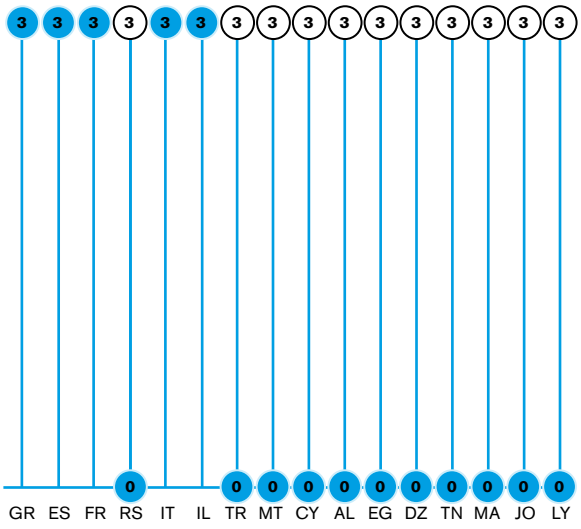


CHART 18 **Cyber Military Units May 2021**



below) published on the NCSI website (National Cyber Security Index), we can confirm that the current state of security is similar to a web-based protective system, which actually looks like a spider's web with many holes and gaps, while what we actually need is a *full-domain cyber dome*.

The AI Environment in the Mediterranean

Current Global Know-how

A global study released in May 2018 by Asgard, a Berlin-based venture capital firm focused on AI, states that by far the country with the largest AI industry is the US (40%), followed by China (11%), Israel (11%) and the UK (7%).[1]
In scientific and military literature, there are countless articles about AI development, describing its possibilities and warning those who fall behind in the AI arms race.

Arms Race

Extensive research by academia and industry is changing the face of modern warfare. The world's superpowers are engaged in an esoteric, pitched arms race on the advances in AI-powered autonomous systems, unmanned arms vehicles, drones, lasers, etc. Military theorists are now doubling down on AI research to turbocharge their country's warfare capabilities.
As nations, individually and collectively, accelerate their efforts to gain a competitive advantage in sci-

[1] *Artificial Intelligence – A Strategy for European Startups, Recommendations for Policymakers*, ASGARD2018, https://asgard.vc/wp-content/uploads/2018/05/Artificial-Intelligence-Strategy-for-Europe-2018.pdf, archived at https://perma.cc/KG2U-R3XX.

Nation state attackers are arguably the most dangerous because they are not driven by emotion or zeal like a terrorist. They are deliberate, calculated, well funded and supported with the resources to target anything they deem worthwhile

ence and technology, further weaponization of AI is inevitable. As a result, the status of "Artificial Weaponized Systems" (AWS) would alter the very meaning of what it is to be human, along with the very fundamentals of security and future of humanity and peace.
Below are examples of current capabilities.

- C6ISR

This powerful AI/ML capability can allow select Mediterranean governments to persistently monitor crises and generate a wealth of actionable intelligence for military and civilian decision makers to proactively engage in responses and anticipate a multitude of threats.
From my personal exposure with this technology, it is the most breathtaking I have seen yet. The technology exists today to deliver a centralized C6ISR system that combines advanced sensors, ISR workflow practices and intelligence tradecrafts and can analyze threats in real time, anticipate and predict threat activity, calculate damage assessment and provide recommended courses of action (COAs).
A real-time virtual machine is at the heart of this process. It will ingest imagery data, geospatial intelligence, signal intelligence reports, cellular phone metadata, real-time video feeds, social media and a variety of other sources. This dynamic system learns from experiences, actions and inputs, and grows increasingly more effective.
Potential situations a C6ISR can help with are; counter-insurgency/terrorism, political unrest and public dissatisfaction, political coups and regime change attempts, cyber defence/offence, support to conventional land, air and sea operations, border conflicts, drug interdiction, illegal cross-border smuggling and disaster management.

- Lethal Autonomous Weapons (LAWS)

These are AI-powered autonomous weapons systems, known as force multipliers for future warfare. Currently, the armies and defence departments of several nations are on their way to deploying autonomous lethal AI systems called Lethal Autonomous Weapons (LAWS).
LAWS are highly sophisticated AI-powered weapons that use sensors and artificial intelligence to identify and destroy targets. They can select and engage targets based on a set of predetermined criteria.

- AI-Enabled Drones

With each passing day, drones are gaining more autonomy. AI-enabled weapons systems such as armed drones selectively target threats, causing less collateral damage. A case in point is the Chinese attack drone, Blowfish A2,[2] unveiled by Ziyan UAV at the 2019 LIMA exhibition.

- AI-Powered Killer Robots

Researchers worldwide are developing killer robots, which can carry out attacks without human intervention and can help in target identification and classification.

The Mediterranean's AI Environment

- EU (North Mediterranean)

Margrethe Vestager, Executive Vice-President of A Europe fit for the Digital Age, said: *"On Artificial Intelligence, trust is a must, not a nice to have. With these landmark rules, the EU is spearheading the development of new global norms to make sure AI can be trusted. By setting the standards, we can pave the way to ethical technology worldwide and ensure that the EU remains competitive along the way. Future-proof and innovation-friendly, our rules will intervene where strictly needed: when the safety and fundamental rights of EU citizens are at stake."*

[2] According to sources, the attack drone can carry radar-jamming devices, guns or bombs under its spine. Later, the company introduced Blowfish A3, which can carry multiple types of machine guns and features a different aerodynamic design allowing the gun to shoot at more angles mid-flight.

- MAGHREB (South Mediterranean)

The Maghreb countries (Tunisia, Algeria and Morocco) are working on national artificial intelligence strategies. The embryonic AI ecosystems forming in all three countries are at varying degrees of maturity. While awaiting the development of such strategies, governments have already started to launch various initiatives to prepare their countries for this new technological revolution.[3]

Concluding Remarks

Current discussion around the impact of AI/ML on national security strategy is focused on the operational level of war. This includes how future wars will be influenced by new military capabilities, and how those capabilities will, in turn, influence conflict on the battlefield.

At the operational level, we need to consider how artificial intelligence will influence ethics in national security. Particularly the role played by decision-makers, i.e., how much autonomy they have in employing force, and how much they delegate to a machine.

Cyberspace is turning into a theatre for geopolitical interactions. Multiple cases, such as those seen in Libya and Syria, have turned into digital battlegrounds, with foreign actors exacerbating the ongoing conflicts with cyber attacks, propaganda and disinformation.

As states use aggressive AI-driven strategies, opponents will respond ever more fiercely. As with all weapons, the use of AI-driven operational plans is escalating. This could evolve into ever more devastating cyber attacks on critical infrastructure and economic production facilities. Such a vicious cycle might ultimately lead to a physical deployment and morph into conventional warfare.

Criteria are needed to determine proportional responses, as well as to set clear thresholds for distinguishing "act-of-war" cyber attacks. In each case, a unilateral approach will be ineffective. Rather, a collective doctrine must be defined for state action in cyberspace. Alarmingly, international efforts to regulate cyber conflicts have stalled. The TALLINN manual is an approach and an encouraging start, if it is edited further to include AI.

Mutually beneficial capacity-building initiatives must be at the forefront of Mediterranean cooperation. Discussing ways to improve and strengthen cybersecurity posture and resilience should be a priority for the MED North-South region, with outdated security precautions being targeted by cybercriminals and nation state actors.

The absence of a legal framework in relation to cyberspace warfare provides attackers with a disproportionately large amount of cover and plausible deniability. This uncertainty is giving organized crime groups, hacktivists and nation states added flexibility that is not sustainable in the future of warfare.

As states use aggressive AI-driven strategies, opponents will respond ever more fiercely. As with all weapons, the use of AI-driven operational plans is escalating. This could evolve into ever more devastating cyber attacks on critical infrastructure and economic production facilities. Such a vicious cycle might ultimately lead to a physical deployment and morph into conventional warfare

Cyber diplomacy goes hand-in-hand with building capacities. Strengthening multilateral coordination and openly communicating efforts and best practices is productive.

Moving forward into the Mediterranean Battlefield

We need to be ready to respond to large-scale, cross-border cyber attacks and cyber crises. Cross-border

[3] *Mapping the AI Maghreb country's ecosystem*. UNESCO report December 2020.

interdependencies means the need for effective cooperation between Euromed states, for faster response and proper coordination of efforts at all levels. This entails:

— Creating a cyber defence committee for good governance and increasing the number of joint exercises designed to respond to attacks through international cooperation, dialogue, capacity building and joint investigations.
— Exchanging different cyber defence-related information and assistance to improve cyber incident prevention, resilience and response capabilities by setting up a multi-agency Computer Emergency Response Team (CERTs).
— Adopting a cyberwarfare treaty, (similar to the EU cybersecurity act), with objectives to reinforce trust and enhance cooperation between Euromed Member States

World leaders, including Obama, Xi and Putin, have all made important statements that bring to the forefront the significance of AI. The Russian President Vladimir Putin stated in September 2017: "Artificial Intelligence is the future for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world."[4]

The absence of a legal framework in relation to cyberspace warfare provides attackers with a disproportionately large amount of cover and plausible deniability. This uncertainty is giving organized crime groups, hacktivists and nation states added flexibility that is not sustainable in the future of warfare

In conclusion, we are collectively facing serious challenges. Cyberwarfare is becoming ever more complex and does not respect borders. The southern Mediterranean region is badly equipped compared to the North. We must, therefore, put in place a common C6ISR system as a tool of war based on common trust.

[4] "'Whoever leads in AI will rule the world': Putin to Russian children on Knowledge Day," RT, 1 September, 2017, www.rt.com/news/401731-ai-rule-world-putin/