FULL-SPECTRUM WARFARE
- FROM BROADENING THE INSTRUMENTS TO THINKING THE UNTHINKABLE -

Professor Iulian CHIFU, PhD[*]

Cosmin GRIGORE, PhD Student[**]

Centre for Conflict Prevention and Early Warning, Bucharest

DOI: 10.55535/RMT.2025.2.01

Full-spectrum warfare has emerged as a new concept, occupying a space between hybrid, asymmetrical, and irregular warfare, although it is not fully aggregate in the epistemological realm. Present in several military strategies and documents from Australia, the USA, Russia, and China, it migrated into a family of concepts related to full-spectrum dominance, full-spectrum instruments or full-spectrum defence. The most important part of its content is linked to surprise and unexpected evolution as well as to creative and innovative elements in the family of thinking the unthinkable and unknown unknowns. We are conducting integrated research on the concept and establishing an operative definition based, also, on a number of concrete applications in the real operations developed by Israel, Ukraine, Russia, USA nowadays.

The methodology used in this approach includes an epistemological debate and the identification of the unique features that gave broad spectrum warfare its specific and added value, as well as a full encyclopaedic debate on the significance of the concept in question.

Keywords: unknown unknowns; thinking the unthinkable; full-spectrum warfare; surprise; unexpected evolution;

[*] Professor "Carol I" National Defence University, Bucharest, Adjunct Professor, National University of Political Sciences and Public Administration, Bucharest.

[**] PhD Student, National University of Political Sciences and Public Administration, Bucharest.

INTRODUCTION AND METHODOLOGY

The current turmoil and unpredictability in international relations, security studies, and the World Order need more and more instruments of investigation and a new approach to defining and explaining, if not anticipating, strategic surprise (Chifu, Simons, 2023). Several elements are developed in prospective studies (Chifu, 2022) and we are maintaining the added value that the concepts of unknown unknowns and thinking the unthinkable, as well as the references that the black swan events (Taleb, 2010) and similar associated concepts are bringing into the debate. The solution was to introduce, based on a number of evolutions in the practical operations conceived, the concept of *full-spectrum warfare* allowing us to introduce all means, military and non-military, as well as instruments rarely associated with conflicts and violence, like corruption, cognitive operations or subversion in times of peace.

Discussing the limits of prediction and the model of prospective studies proves to be, in fact, instrumental to make the epistemological distinction between the full spectrum warfare and related concepts like hybrid, irregular, asymmetrical, non-kinetic warfare, and so on.

Discussing the limits of prediction and the model of prospective studies proves to be, in fact, instrumental to make the epistemological distinction between the full spectrum warfare and related concepts like hybrid, irregular, asymmetrical, non-kinetic warfare, and so on. Moreover, the concept evolved in several documents, with different significance that needed to be identified and clarified. This article aims to clearly define the suitable and mandatory traits of full-spectrum warfare in order to represent, at an epistemological level, a useful term and concept to be used in security studies.

Our methodology comprises an epistemological debate and the identification of unique traits that have given full-spectrum warfare its specific and added value, as well as a full encyclopaedic debate on the significance of the concept at hand. The focus on surprise, unknown unknowns, and thinking the unthinkable provides us with the necessary space to identify the fields where the full-spectrum warfare is developed and the acceptability of all instruments at hand for creating the strategic surprise, even in a one-time attack.

Common coordination and integration of all tools in planning full-spectrum attack, defence, or aggression is also an integral part of the content of our concept. That is the way 21st century conflict is developing (Simons, Chifu, 2017).

UNKNOWN UNKNOWNS, THINKING THE UNTHINKABLE

Unknown unknowns, the formula becoming a concept, is attributed by everyone to Donald Rumsfeld who mentioned it, on 12 February 2002, in a briefing at the Pentagon (DoD News Briefing, 2002). In fact, it is only the famous part of the triad of known knowns, known unknowns, and unknown unknowns. Donald Rumsfeld said: *"Reports that a certain thing did not happen are always interesting to me, because, as you know, they are knowns; there are known knowns. We also know that there are known unknowns; this means that we know that there are certain things we do not know. But there are also unknown unknowns – the ones we don't know we don't know about. And if someone looks at the history of our country and other free countries, only this last category represents the really difficult elements"* (Ib.).

"Reports that a certain thing did not happen are always interesting to me, because, as you know, they are knowns; there are known knowns. We also know that there are known unknowns; this means that we know that there are certain things we do not know. But there are also unknown unknowns – the ones we don't know we don't know about."

But the *unknown unknowns* term was used in NASA[1] and, along with known unknowns, both are commonly used in project management and strategic planning (Courtney, Kirkland, Viguerie, 1997). Trung Ank Dang name unknown unknowns – things or phenomena that we do not realize exist or understand (Trung Anh, 2002), things, phenomena or evolutions that we do not even know are there to try to find out something about them, or unidentified things that we do not know that we should know in order to react. David C. Logan reviewed the triad of terms in the context of general scientific research, biology, in this particular case (Logan, 2009, pp. 712-714).

Unknown unknowns are things we did not even know how to look at and did not know that we were missing or needed to be researched. As scientific research evolves, there is a phenomenon by which the unknown unknowns turn into unknown known ones. We are aware

[1] See the hearings on 24-25 June 1981 that took place in the Commission for Science and Technology of the House of Representatives of the US Congress, https://books.google.be/books?id=dRMrAAAAMAAJ&pg=PA73&dq=%22unknown+unknowns%22&hl=en&sa=X&ved=0ahUKEwjhnraJ-7XmAhVGi1wKHUi0Bl0Q6AEIKTAA#v=onepage&q=%22unknown%20unknowns%22&f=false, retrieved on 22 May 2025.

of their existence and the need to investigate them, to take them into account, and to consider them. And this component falls within the scope of scientific discovery, even if it does not contain, at this stage, the component of scientific research (Chifu, 2002).

Hugh Courtney and his team (Logan, ib.) linked the concept to the dangers of a situation of uncertainty for decision-makers. Underestimating uncertainty is just as bad as assuming a completely unpredictable world: a sufficiently clear future, existence of alternative futures, a spectrum of future scenarios, and the full ambiguity, unknown unknowns, with several dimensions of unpredictability that intersect and influence each other and the result is impossible to predict in the environment and with the available indicators. We must accept the limits of knowledge and the fact that the future scenario may be impossible to identify, much less predictable, all relevant variables being, in turn, unpredictable and overlapping, with a random result.

Underestimating uncertainty is just as bad as assuming a completely unpredictable world: a sufficiently clear future, existence of alternative futures, a spectrum of future scenarios, and the full ambiguity, unknown unknowns, with several dimensions of unpredictability that intersect and influence each other and the result is impossible to predict in the environment and with the available indicators.

In 2012, Nigel Walpole launched the debate on **thinking about the unthinkable** in the fight between the Royal Air Force and the pilots of the East German forces during the Cold War (Walpole, 2012). This type of thinking has older origins, the unthinkable in the context of the opponent's nuclear actions, and Herman Kahn was the one who engaged in the analysis, description, and planning of the prospect of a nuclear war (Kahn, 1985). But the most important theoretical contribution and the launch in a contemporary context of the concept of thinking the unthinkable – with all the substratum and substance of a concept in the full force of the word – came from Nik Gowing, discussing the limits and difficulties of leadership in predicting and avoiding unexpected developments (Gowing, Langdon, 2015). Subsequently, together with an entire team, he launched in 2016 a website and a project called *Thinking the unthinkable* in support of political leaders, in fact, decision-makers (https://www.thinkunthink.org/). He prefaced the book of the same name published in 2018 (Gowing, Langdon, 2018).

Chris Donnelly opens another line of thought, linking instability and turbulence to the prospect of war. He clearly notices the limit of the institutional capacity for anticipation and prevention. So, the excessive presence of the unthinkable in the contemporary era is, for him, a sign of the approach of a form of war: "*The level of change we are facing*

at the moment is comparable to what happens in times of war. We have changes during wartime, even though we believe we are at peace. The global dimension of change exceeds the capacity of national and international institutions", says Chris Donnelly (Donnelly).

Thinking the unthinkable is related to nine reasons for limitation in decision-making and anticipation:

1. overwhelming of decision-makers with intense and multiple pressures;
2. institutional compliance;
3. deliberate blindness;
4. groupthink – compliant group thinking;
5. risk aversion;
6. fear of career-limiting movements;
7. reactionary thinking systems;
8. denial;
9. dissonances and cognitive overload (Gowing, Langdon, 2018).

Thinking the unthinkable is related to nine reasons for limitation in decision-making and anticipation: overwhelming of decision-makers with intense and multiple pressures; institutional compliance; deliberate blindness; groupthink – compliant group thinking; risk aversion; fear of career-limiting movements; reactionary thinking systems; denial; dissonances and cognitive overload.

THE CONCEPT OF FULL-SPECTRUM WARFARE

We will build up the concept based on three categories of instruments: the definition attributed to the concept (and its evolution), the related concepts, and the official documents using this concept. Then we will de-construct the major characteristics and propose an operational definition. After this endeavour, we will discuss relations with similar concepts and identity nuances associated to full-spectrum warfare. In that sense, full-spectrum warfare has a direct relationship with the full spectrum defence, requiring the defence against all instruments and components of a full-spectrum warfare. Full-spectrum dominance is the capacity of protecting, preventing, reacting and eliminating the threat and aggression on each of the components of full-spectrum warfare.

Full-spectrum warfare is not only about summing up or integrating different instruments tailored to respond to a certain type of aggression or threat. It is about a common command and control, common planning, with needed sensors and early warning systems, that could react altogether to a complex full-spectrum warfare attack that combines, at the same time, those instruments situated in different spectrums and coordinated through the original planning of the attack.

It integrates and coordinates and does not maintain dispersed the type of counter-weapon of choice for each and every type of attack or spectrum where the attack is taking place.

We have several definitions and approaches to the full-spectrum warfare. **Full-spectrum warfare** encompasses **a wide range of integrated military and non-military means of state power and clandestine actions available to a hybrid actor** (Abdyraeva, 2020). The US military defines full-spectrum dominance as the control of all the physical domains of the earth – from the seas to the skies, meaning a definition closer to a multidomain approach – terrestrial, maritime, atmospheric, and extra-terrestrial spaces – by a sophisticated war machine (Shaw, 2016). The term expresses **the spheric dimension of human security more generally**. To be safe and secure is to be housed within an enclosure, some kind of dome that protects its inhabitants from the outside. The final frontier of military enclosure and, in many ways, the end game of full-spectrum dominance is the occupation of outer space with spy satellites and other orbital weapons.

Full-spectrum warfare encompasses a wide range of integrated military and non-military means of state power and clandestine actions available to a hybrid actor.

So, for the US, **full-spectrum dominance** is a military concept – or ambition – for the total occupation and control of land, sea, outer space, cyberspace, and even psychological space (Ib.). The ultimate objective was *"full spectrum dominance"*: preponderance across the entire spectrum of warfare from conventional conflicts through to irregular war (Joint Chiefs of Staff , 2004). This phrase was also used during the Clinton years but did not refer to irregular warfare; instead, it referred to the stages of conflict from peace through to conventional war (Ryan, 2001), which calls for *"conventional warfighting capabilities… across the full spectrum of military operations"*.

Rumsfeld wanted the military to develop *"a portfolio of key military capabilities"* that would enable it to confront a spectrum of threats rather than planning only for one particular type of conventional adversary (Rumsfeld, 2001), planning for victory across the spectrum of possible conflict (Ib., p. 18). The military understanding was also niched into the anti-terrorist and irregular warfare (Chiarelli, 2005).

In the same area of multidomain thinks Australia in its documents: full-spectrum defence is an integrated, five-domain military strategy that exploits Australia's technological strengths and unique ability to leverage off the still-dominant communications, intelligence,

and space-based capabilities. Australia should develop and pursue a ***"full-spectrum"* military strategy** in recognition of the need to provide protection against military threats emanating from outer space and cyberspace, as well as the land, sea, and air (Dupont, 2015).

Russia has less theorized, but has applied a Full Spectrum Conflict: Russian warfare was approached from the **four spectrums** of military, information, economic, and energy, and from political influence operations. From this, Jonsson and Seely proposed the concept of **Full-Spectrum Conflict** that captures the use of violent and non-violent means as well as the conduct of conflict in differing degrees of intensity from peace to war and the space in between (Jonsson, Seely, 2015). They are the ones realizing the need for centralized and unique control for all operations coordinated in a full-spectrum conflict: several military and non-military means are under one central command and directed to the same political goal. This is noteworthy because a number of means, for instance, food sanctions and the broadcasting of biased news, would be excluded while insisting on a strict definition of warfare (Ib.).

We consider full-spectrum warfare a wide range of military and non-military means, used by state or non-state actors, in a coordinated and integrated planned operation, with the objective of developing a surprise action and create a strategic advantage through unexpected series of events, both benign and legal and maligned and illegal, involving as well aggression and violence.

The same suggestion of a common command comes in the study of the Chinese approach to the Three Warfares (Reichborn-Kjennerud, Cullen, 2016). To quote one US DoD report, Chinese *"Three Warfares"* is challenging for the USA because it is a concept executed by an organization (the General Political Department) that has no analogue in the USA (Halper, 2013). Without such an office, or a political mandate, or even a philosophical understanding that warfare operates in a coordinated fashion along the full-spectrum of civilian and military space, Western coordination of a response to full-spectrum warfare becomes complicated (Reichborn-Kjennerud, Cullen).

OPERATIONAL DEFINITION

So, in our operational definition, we consider **full-spectrum warfare** a wide range of military and non-military means, used by state or non-state actors, in a coordinated and integrated planned operation, with the objective of developing a surprise action and create a strategic advantage through unexpected series of events, both benign and legal and maligned and illegal, involving as well aggression and violence.

So, our epistemological rationalization kept into the definition of integrated and coordinated approach, surprise, and full-spectrum instruments, including civilian benign and legal components that become illegal in association with the planning and achievement of the full-spectrum attack.

HYBRID, ASYMMETRICAL, IRREGULAR WARFARE – THE DIFFERENCES IN MEANING

We need to separate the current full-spectrum warfare concept from the existing ones of irregular, asymmetrical, hybrid warfare. First, there is a clear difference from irregular warfare, once the aim exceeds the irregular part, as well of asymmetry between the parties involved. Yes, the attacker could be a non-state actor, even a terrorist or insurgent actor, but the full-spectrum warfare exceeds that level of military conventional violence as well as the military means (including IED). And, it could be used (and it is used in practice) by the state actors against state actors, as we could see in the practical examples in the last part of our article.

The most complicated part is to make the difference in identity between the concept of hybrid warfare and full-spectrum warfare. And it leads also to making the differences between the conventional and hybrid warfare, since full-spectrum warfare comprises both military and non-military means, therefore accepting that conventional and hybrid warfare are part of the full-spectrum warfare, but it also includes legitimate and civilian unconventional means like corruption, using criminal instruments, recruiting blindly civilians. As the utilitarian way of defining hybrid warfare was warfare open to indefinite *"ways and means to achieve an effect"* (Ib., p. 1), a definition which is intended to enhance an overall generalization of the concept and also simultaneously to increase its applicability, we need to see how this works for full-spectrum warfare.

The scope of tools and techniques available to hybrid warfare actors for the achievement of their particular objectives – political, economic, societal, informational – has, in turn, also significantly broadened with the evolution of information technologies and the rise of non-state actors such as hacktivists, who challenge nation-states by strategically targeting vulnerabilities of governmental websites.

The scope of tools and techniques available to hybrid warfare actors for the achievement of their particular objectives – political, economic, societal, informational – has, in turn, also significantly broadened with the evolution of information technologies and the rise of non-state actors such as hacktivists, who challenge nation-states by strategically targeting vulnerabilities of governmental websites.

A distinctive feature of cyber activities is that they can be carried out clandestinely and covertly. As a result, states can potentially lose a war before even knowing that it has already begun (Abdyraeva). The clandestine and covert operations are thus added to the hybrid warfare.

Besides hacktivism, social media is another important instrument of hybrid warfare as it can equally be employed as a *"weapon"*. This again reinforces a central idea behind the hybrid warfare as states use weaponized information to *"deploy in a rapid-fire series of mutually-reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal cost"* (Herrmann, 2017). So all of those elements are part in the hybrid warfare, but some are added for a full-spectrum warfare: coming from nuclear, conventional components, at the end of the full spectrum, going to real full-scale military conventional war, and continuing with means like the ones referring to cognitive, information warfare (Chifu, 2025; Simons, Chifu, 2025) and civilian non-conventional means, usually not included in the definition of warfare since they do not hold elements of violence or direct aggression except in combination with other means, as it is the case for achieving surprise in a full- spectrum warfare.

Besides hacktivism, social media is another important instrument of hybrid warfare as it can equally be employed as a "weapon". This again reinforces a central idea behind the hybrid warfare as states use weaponized information to "deploy in a rapid-fire series of mutually-reinforcing stories that are hard for people to disregard and reach a global audience in seconds at minimal cost".

For a full debate, we also need to clarify the relationship between hybrid and conventional warfare. Conventional warfare can be conducted by using any conventional weapons and is primarily waged against the adversary's military forces in an open confrontation. In contrast to the conventional regular warfare, the hybrid warfare is a mix of both conventional and unconventional warfare that simultaneously combines the use of *"conventional capabilities, irregular tactics and formations, and terrorist acts including indiscriminate violence, coercion, and criminal activity"* (Hoffman, 2007, p. 8). Accordingly, the use of force can be defined as *"hybrid"* as long as warfare is not conducted one-dimensionally through purely military means or non-military tools that are available to a state or non-state hybrid actor (Abdyraeva).

Therefore, some definitions of hybrid warfare can contain the conventional military part of the spectrum, except that nuclear instruments are completely ruled out. As well as civilian non-aggressive

instruments that will never be considered warfare. Surprise, integrated and coordinated means, and political mandate are also making the difference between hybrid and full-spectrum warfare.

THE HISTORICAL EVOLUTION

We have seen the source of inspiration in developing the full-spectrum warfare. The USA, after 9/11, tried to developed capabilities to fight any type of attack and defines full spectrum defence and dominance. Total defence from threats and attacks coming from outside the territorial limits was developed afterwards with the Reagan-era global missile shield, the so-called **Star Wars system**, which was meant to protect the American continent from Soviet missiles during the *Cold War*. Anti-ballistic shield for the USA and NATO countries came naturally. Relatedly, consider Israel's more recent **Iron Dome anti-rocket system**. The dome is thus a cartographic design for an atmospheric form of security, an enclosure that protects against horizontal and vertical intrusions, putting a roof – electromagnetic or otherwise – above our heads (Shaw). The new **Trump Golden Dome** as well as the announced Turkyie Iron Dome are part of the same reality.

Total defence from threats and attacks coming from outside the territorial limits was developed afterwards with the Reagan-era global missile shield, the so-called Star Wars system, which was meant to protect the American continent from Soviet missiles during the Cold War.

The US military is attempting to install **a three-tiered *"space shield"* that envelops the earth within a totalizing surveillance network**. From satellites in the exosphere to space-based aircraft in the upper stratosphere to drones swarming in the lower stratosphere, the weaponization of the atmosphere is crucial to the future. This is how the world is becoming **an electronic battlespace.** *"The military recognizes that success in any future European conflict will depend to a large extent on **mastery of the electromagnetic spectrum**"* (Aviation Week and Space Technology, 1974, p. 57). **Cyberspace** is a **crucial domain for full spectrum dominance** and enables the kind of bulk surveillance. Therefore, **a globalized battlespace in a project of full-spectrum dominance** (Shaw).

Australia had its own history that led to the definition of full-spectrum warfare. First it came from its geographical position and propension to rely only on maritime capabilities. In place of a maritime strategy, Australia needed to adopt a *"full-spectrum"* approach to defence that can provide protection against military threats from outer

space and cyberspace, as well as the conventional domains of land, sea, and air (Dupont). **Full-spectrum defence** must be underpinned by deeper and broader regional defence partnerships and by a risk assessment process that encourages critical thinking and the future capabilities of the Australian Defence Forces.

Australia's defence strategy had two main purposes: to help shape the regional and international security environment in support of a rules-based, liberal democratic order; and to deter and, if necessary, defeat armed attacks against the nation's territory, people and vital interests[2]. It was a persisting illusion that geography provides Australia with *"immutable"* and *"abiding"* strategic benefits[3]. But **distance and location are far less of a barrier today** because globalization is continuing to **shrink physical space at an ever-accelerating rate**. A former Chief of Navy has argued for a maritime *"third way"* between the **continentalist and the expeditionary traditions of Australian strategic thinking**[4].

The ability to project military hard power a long way from the Australian continent is entirely consistent with territorial defence, Australia's alliance obligations, and established reputation for good global citizenship. That is how Australia has reached the understanding that it needs a "full-spectrum" military strategy in recognition of the need to provide protection against military threats emanating from outer space and cyberspace, as well as the land, sea, and air.

Even **the concept of strategic warning**, which has become *"a crucial element of defence planning"*[5], proves not to be enough in an era of **complex, transnational challenges and messy, irregular conflicts** which can arise at extremely short notice. It would be dangerous to believe that our intelligence community can be relied upon to **provide timely warning of significant threats**. Even the best intelligence has its limits. As the 2013 Defence White Paper acknowledges, **the ability to project military hard power a long way from the Australian continent** is entirely consistent with territorial defence, Australia's alliance obligations, and established reputation for good global citizenship (Defence White Paper, 2013, pp. 29-30). That is how Australia has reached the understanding that it needs **a *"full-spectrum"* military strategy**

[2] With minor variations, these two objectives have been an enduring and largely unremarked feature of Australian defence strategy since the 1976 Defence White Paper, attracting little criticism or debate.

[3] Department of Defence, *Defence White Paper 2013: Defending Australia and its National Interests*, (Canberra: Commonwealth of Australia, 2013): 30; Department of Defence, *Defence 2000: Our Future Defence Force*, (Canberra: Defence Publishing Service, 2000): 23; Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, (Canberra: Commonwealth of Australia, 2009): 49.

[4] *Defence White Paper 2013*: 29-30 and Vice Admiral Ray Griggs, Chief of Navy, *"The Navy's Role in the Maritime Century"*, (speech, Lowy Institute for International Policy, Sydney, 17 August 2012), http://www.lowyinstitute.org/files/griggs_- _the_navy_in_the_maritime_century.pdf).

[5] *Defending Australia in the Asia Pacific Century: Force 2030*: 27.

in recognition of the need to provide protection against military threats emanating from outer space and cyberspace, as well as the land, sea, and air (Dupont).

The Australian Government did not stay in the multidomain type of definition but extended full-spectrum warfare by acknowledging, in its 2009 White Paper, that new **disruptive technologies that could threaten network capabilities were likely to increase**, and that the **threat and complexity of cyber warfare** were also likely to increase (Ball, Watters, 2013). The 2013 White Paper includes **security against major cyber-attacks on Australia beyond the capacity of civilian agencies to counter**, as part of the defence of Australia against direct armed attack, Australia's most basic strategic interest[6]. The White Paper addresses **electronic warfare and UAVs** but does not attempt to bring them together with cyber considerations into any sort of operational planning construct.

In the case of Russia, we have seen **four spectrums of military, information, economic, energy, and from political influence operations** (Jonsson, Seely). Equally important is that the arena for the **information war is changing**. The expansion of social media enables not only **instantaneous news consumption and distribution** but also crowdsourcing, **enabling mass manipulation across the information spectrum**, from state-directed media to paid trolls attacking anti-Russian positions (Weil, 2010).

And Russia took advantage to develop cognitive and information warfare against the West. Its operations are developed in an aggressive constant stance, with **differing degrees of ambiguity and intensity.** As a characteristic, however, **the Russian conduct of full-spectrum conflict is still partly one of physical violence.** When **more subtle forms of violence – subversion and diplomacy – are insufficient for Russia to reach its political goal, the amount of violence is modulated.** In this light, applying kinetic violence is the means of **last resort in the conduct of full-spectrum conflict**, the constant threat underpinning all the other means (Jonsson, Seely).

When more subtle forms of violence – subversion and diplomacy – are insufficient for Russia to reach its political goal, the amount of violence is modulated. In this light, applying kinetic violence is the means of last resort in the conduct of full-spectrum conflict, the constant threat underpinning all the other means.

A new element in the information spectrum in Ukraine has been the online efforts of **hired commentators and bloggers, *"trolls"*,**

[6] Commonwealth of Australia, *Defence White Paper 2013* (Canberra: Department of Defence, 2013, para 3.9.

to post pro-Kremlin comments on the Internet. A document leaked from Agenstvo Internet-Isledovaniy (Internet Research Agency) to BuzzFeed outlines how the Agency uses its $19 million budget to employ 600 people whose daily tasks included commenting on 50 news articles, managing six Facebook accounts with three posts a day, managing 10 Twitter accounts, and tweeting 50 times a day (Seddon, 2014).

DOMAINS AND CONTEXT FOR A FULL-SPECTRUM WARFARE

There are several systems of instruments in a full-spectrum warfare. In one case, those conventional military and hybrid activities are:

- ❖ Economic disruption
  - Economic sanctions
  - Leveraging and using natural resources as a foreign policy tools
- ❖ Strategic Weaponization of Information
  - Propaganda and disinformation campaigns:
    - Δ Sponsoring news outlets:
      - a) To spread fake news
      - b) To spread conspiracy theories
- ❖ Social media manipulations:
  - Using troll farms, advertisements, bots to spread polarizing messages
- ❖ Cyber Operations
  - Cybercrime:
    - Δ Hacks into critical infrastructure, political organizations
- ❖ Politicians
- ❖ Cyber espionage:
  - To gather intelligence
  - To strategically leak private information
  - To alter stored information
- ❖ Social/Psychological Manipulation
- ❖ Supporting local upheavals
- ❖ Gaining local support

- ❖ Exploiting social cleavages, nationalist identities, and much debated topics over controversial policies
- ❖ Irregular forces
  - Terrorists, Guerrilla Fighters, Insurgents, Unmarked soldiers
- ❖ Regular military forces
  - Army, Navy, Air Force (Abdyraeva).

Just **how far to extend the concept of hybrid warfare, part of full-spectrum warfare, to include the full spectrum of conflict** without denuding it of its utility – or breaking the meaning of war by slipping into a broader discussion of coercion and competition – is still an open and heated question debate. There are two models for using instruments of power, the MPECI – military, political, economic, civilian, and informational and the aim is PMESII – political, military, economic, societal, informational, and infrastructure vulnerabilities of a target system, to escalate – vertically and horizontally – to achieve the desired goals (Reichborn-Kjennerud, Cullen). Full-spectrum is characterized by the tailored use of all instruments of power against the vulnerabilities, centres of gravity, and critical functions of the opponent's system, in a **synchronized and coordinated fashion**.

There are two models for using instruments of power, the MPECI – military, political, economic, civilian, and informational and the aim is PMESII – political, military, economic, societal, informational, and infrastructure vulnerabilities of a target system, to escalate – vertically and horizontally – to achieve the desired goals.

One of the most distinctive features of the initial operation in Crimea was the coordination between **all military and non-military means**, ranging from the political-strategic to the tactical. The skilful implementation of instruments from the spectrums of **Diplomatic, Economic, Military, and Information (DIME)** is indeed what Norberg, Westerlund, and Franke at the FOI argued to be the only element that qualifies as new (Norberg, Westerlund, Franke, 2014, pp. 41, 48). The concept of **Full-Spectrum Conflict** (FSC) that applies to Russia includes asymmetric, hybrid, and non-linear and captures both the multitude of means involved, **from *"conventional"* military units to clandestine special forces and intelligence operatives**, to hybrid means, like the **economic threats, political influence, online and offline information battles, as well as *"traditional"* subversion.** Here some will say is applicable the word conflict rather than war or warfare, since **many of these means are non-violent in character**, and the standard Western way of understanding war is violence in the blast and fragmentation sense of the word (Clausewitz). This concept

importantly captures that these means do take a part in a fundamental clash of wills.

A special place should be devoted to the drone war since it is the most present and impactful in the wars of the 21st century. When the violent use of armed drones is described as *"drone warfare"*, this is usually done without consideration of **what makes violence count as *"war"***. **All war is violent, but not all violence is war**, so not all drone violence will be drone warfare. It is important to be confident, in conceptual terms, about the true nature of violence. When and why **drone violence can plausibly be conceptualized as warfare**. Here, the mutual experiencing of physical risk is arguably a critical factor because war is by nature a contest between contending belligerents (Enemark, 2023).

A special place should be devoted to the drone war since it is the most present and impactful in the wars of the 21st century. When the violent use of armed drones is described as "drone warfare", this is usually done without consideration of what makes violence count as "war". All war is violent, but not all violence is war, so not all drone violence will be drone warfare.

In seeking to **determine when (if ever) drone violence counts as drone warfare**, a useful starting point is to think more generally about the essence of *"war"*. Once the idea of **allowing governments to determine war's existence subjectively and self-interestedly** is rejected **(**Brooks, 2016), conceptualizing an instance of violence as warfare becomes a matter of **referring to *"objective criteria"*** (Alsont, 2010, para. 46). In the most basic sense, war can be differentiated from other forms of violence by **identifying it as being public and political in nature**. Violence wielded exclusively for **private pleasure** and/or for **a criminal purpose** can thus be deemed unwarlike (Clark, 2015, p. 79).

Remotely Piloted Aircraft (RPA), also known as Unmanned Aerial Vehicles (UAV) support to Close air support (CAS) emphasizes **winning today's battles and minimizing friendly casualties by supporting troops in contact** (Fowler, 2014, pp. 108-119). In this role, the RPA can act as both a CAS platform and as a **Forward Air Controller-Airborne (FAC-A)** (Slessor, 1936; Pape, 1996). On the other end of the airpower spectrum is targeting **the enemy leadership with the goal of winning the campaign via decapitation** (Warden III, 1995, pp. 40-55). Targets could be far more extended including lines of communication and infrastructure as well as tactical targets closer to the front lines of battle.

Here another debate is developed about how to use drones since an individual OPV **is not intended to operate alone in high-end**

warfighting. Rather, it is intended to operate as **part of a *"swarm"* or team**. Each OPV would host its own toolbox of a mini-swarm of unmanned and autonomous systems, but the OPVs would also congregate to form larger teams as necessary. A **common control system (CCS)** could be a **key enabler of the mature system of distributed lethality** (Hellyer, 2020). Electronic warfare is also a part of the full-spectrum warfare since frequencies are contested for by both CIS (communication and information systems) and EW (early warning) systems (Palin et al., 2021, pp. 73-79).

We added our own instruments marking the use of corruption and bribes as well as those of criminal instruments to fill the full spectrum (Chifu, 2022, vol. 2, 1.5). Using corruption, the Kremlin does not need to be the leader of a bloc of nations like the Warsaw Pact. Instead, it exacerbates divisions, undermines international institutions, and helps create a world in which its corrupt authoritarianism can flourish. It is about controlling economic and financial structures with opaque schemes, especially energy, at the level of the post-Soviet space, but not infrequently operating in Europe, even if the real owner is hidden under offshore formulas or companies registered in third European countries (Pomerantsev, Weiss).

Using corruption, the Kremlin does not need to be the leader of a bloc of nations like the Warsaw Pact. Instead, it exacerbates divisions, undermines international institutions, and helps create a world in which its corrupt authoritarianism can flourish.

Putin's Russia uses interference, blackmail, and corruption in the legal systems of European states at the political level and in the economic and business structures of these states (Zâgar, 2017). One such illustrative case is the Kalinin-Kurchenko-Babakov case. And the revelations came after Kalinin's capture in Greece and his detention on 28 February – 2 March 2021, after he was put on the wanted list[7], but also his untimely release on 6 March, based on the Putin's people intervention, of Alexander Babakov to Russia's Ceaika attorney general. Russia's interference in the Greek justice system becomes evident through a series of *"coincidences"* and interventions at the highest level (Michalopoulos, 2018). The arrest of Evgeny Kalinin by the Greek authorities was a legitimate one. The Greek authorities

[7] *Ex-top manager of fugitive oligarch Kurchenko's firm detained in Greece upon Ukrainian request*, UNIAN Information Agency, 3 March 2019, https://www.unian.info/politics/10466625-ex-top-manager-of-fugitive-oligarch-kurchenko-s-firm-detained-in-greece-upon-ukrainian-request.html, retrieved on 2 May 2025.

released Kalinin[8], who immediately arrived in Russia, sheltered by arrest warrants and international prosecution. It is no coincidence that Kalinin's release took place on the same day that Russian Attorney General Yury Chaika met the Greek Minister of Justice[9].

PRACTICAL APPLICATIONS OF FULL-SPECTRUM WARFARE

We have selected five cases where full-spectrum warfare was used, implying the most creative ways of conducting operations in a combined manner.

In the nearly year-long struggle between Israel and Hezbollah related to the war in Gaza, the purported attack seems to be the most recent salvo. It set off the war's worst mass casualty event in Lebanon, which left the nation's healthcare system in ruins: Health Minister Firas Abiad reported that at least 2,800 people were hurt nationwide, primarily from injuries to the hands, face, or stomach. There were at least nine fatalities, but a lot of those hurt could not retake their places in the network.

a. Thousands of pagers used by Hezbollah explode

Hezbollah and Lebanese officials reported that thousands of people were hurt throughout Lebanon on Tuesday, 17 September 2024, when electronic pagers used by the militant group exploded simultaneously at around 3:30 p.m., in what experts said may have been an unprecedented Israeli attack that may have involved sabotaging the devices before they were delivered (Haidamous et al., 2024). In the nearly year-long struggle between Israel and Hezbollah related to the war in Gaza, the purported attack seems to be the most recent salvo. It set off the war's worst mass casualty event in Lebanon, which left the nation's healthcare system in ruins: Health Minister Firas Abiad reported that at least 2,800 people were hurt nationwide, primarily from injuries to the hands, face, or stomach. There were at least nine fatalities, but a lot of those hurt could not retake their places in the network.

The Lebanese Shia militant group Hezbollah utilized Israeli-made walkie-talkies booby-trapped with explosives for ten years before their detonation in a surprise strike in September of this year, according to two former Israeli intelligence officers. Hezbollah was tricked into purchasing thousands of manipulated pagers and walkie-talkies

[8] *Russian businessman wanted by Ukraine freed, lawyer says*, ekatmimerini.com, 7 March 2013, http://www.ekathimerini.com/238390/article/ekathimerini/news/russian-businessman-wanted-by-ukraine-freed-lawyer-says, retrieved on 2 May 2025.

[9] *In Greece, the Russian detainee Kalinin was released at the request of Ukraine*, Teller Report, 7 March 2019, http://www.tellerreport.com/news/--in-greece--the-russian-detainee-kalinin-was-released-at-the-request-of-ukraine-.S1bpqMr0IE.html, retrieved on 2 May 2025.

without realizing they were manufactured in Israel. The attacks claimed thousands of lives and injured dozens more. Lebanese officials reported that although Israel claimed it was designed to target solely Hezbollah members, civilians were also among the victims (Berg, 2024).

b. Mohsen Fakhrizadeh: *"Machine-gun with AI"* used to kill Iran scientist

Iranian top nuclear scientist killed by *"artificial intelligence"* satellite-controlled machine gun, according to a Revolutionary Guards officer. At a ceremony in Tehran, Gen. Fadavi, the deputy commander of the Revolutionary Guards, claimed that a machine gun on the Nissan pickup was *"using artificial intelligence"* and *"equipped with an intelligent satellite system which zoomed in on martyr Fakhrizadeh"*. The automatic weapon *"focused only on martyr Fakhrizadeh's face in a way that his wife, despite being only 25 cm* [10 inches] *away, was not shot"*, according to him. The general maintained that *"in total 13 bullets were fired and all of them were shot from the* [weapon] *in the Nissan"* and that there had been no human attackers on the site. He said that Fakhrizadeh's security guard's head was hit by four bullets *"as he threw himself"* on the scientist (BBC, 2020).

The assassins were probably motivated by the widespread usage of remote weapons in the Middle East. In terms of tactics, they offer a steady, precise firing platform, and remote gunners are more likely to be strategic in their shots because they are not under the pressure of being fired at. In addition, it offers two significant benefits over employing ground-based gunmen. One is that, since there were allegedly at least two carloads of the target's bodyguards, there was little chance of an operative being shot down or taken prisoner in a battle with them. The inability to track the attack is the second benefit. The remote-controlled weapon was found by the side of the road in a Nissan pickup. The Nissan and most likely all the evidence of who carried out the attack were destroyed by a massive bomb after the weapon fired many bursts from a distance of 150 meters, striking Fakhrizadeh multiple times (a bodyguard was also killed). Many countries, including Iran, have chosen to deploy unmanned aircraft instead of manned ones for specific tasks because of this anonymity (Hambling, 2020).

c. Operation Spiderweb: Russian aircraft destroyed by Ukrainian drones

In what Kyiv says is its longest-range attack of the war, a Ukrainian drone attack destroyed billions of dollars worth of Russian aircraft that were based at facilities around the nation, including places as far away as Siberia. Spiderweb was a fantastic operation that took 18 months to organize in secrecy. Before launching them remotely, for a concerted attack meant to target Moscow's air dominance, Ukraine's spies transported explosives and short-range drones into Russia. Drones were brought into Russia illegally and put inside containers, which were then loaded into trucks, according to Vasyl Maliuk, chief of the Security Service of Ukraine (SBU).

In what Kyiv says is its longest-range attack of the war, a Ukrainian drone attack destroyed billions of dollars worth of Russian aircraft that were based at facilities around the nation, including places as far away as Siberia. Spiderweb was a fantastic operation that took 18 months to organize in secrecy.

The trucks were parked close to Russian outposts, and a remotely operated device raised the containers' roof panels so the drones could fly out and launch their assault. The drones might be controlled remotely, most likely from Ukrainian territory, thanks to first-person view (FPV) technology (Mazhulin et al., 2025). Drones can be seen flying from the roof of one of the vehicles in the videos that are making the rounds online. The drivers of the trucks from which the drones took off all related similar tales of being hired by businesses to deliver wooden cabins in different parts of Russia (Gozzi, 2025).

d. Stuxnet

Stuxnet was a computer worm discovered in June 2010 that was specifically written to take control of certain programmable industrial control systems and cause the equipment controlled by those systems to malfunction, while simultaneously feeding false data to the systems monitors indicating that the equipment was operating as intended. To be more specific, on 17 June 2010, an unnamed antivirus firm in Belarus received an email from a customer in Iran stating that a machine was repeatedly resetting itself. This flaw led to the discovery of a mystery piece of malicious software (malware), dubbed *"Stuxnet"* by forensic experts after a file name in the code. Stuxnet has been dubbed *"the most technologically advanced malicious malware built for a targeted attack to date"* and *"a precise, military-grade cyber missile"* by computer security specialists (Lindsay, 2013, pp. 365-404).

Stuxnet was designed to attack Siemens AG's *"supervisory control and data acquisition"* (SCADA) systems, which are used to manage machinery in power plants and other similar installations. The worm exclusively targeted Siemens SCADA systems used in connection with frequency-converter drives, which regulate the speed of industrial motors. Even then, only drives made by certain manufacturers in Finland and Iran were configured to run motors at extremely high speeds.

e. Ayman al-Zawahiri: Al-Qaeda leader killed in US drone strike

President Joe Biden revealed that the United States of America assassinated Ayman al-Zawahiri, the leader of al-Qaeda, in a drone operation in Afghanistan. He was slain in Kabul, the capital of Afghanistan, during a CIA counterterrorism operation (Plummer, Murphy, 2022). In his brief remarks from the White House, President Biden mentioned a drone strike. The drone had dropped two Hellfire missiles, according to an American official who spoke to the media on condition of anonymity, and there had been no need for an American military presence on the ground. Kabul acknowledged that an *"air attack"* had been carried out by *"American drones"*, after first denying a drone strike and citing a *"rocket"* that had struck *"an empty house"* (Favier, 2022).

The Al-Qaeda leader's family was in the house, but there were no signs of an explosion on the targeted structure or collateral casualties. All of these hints suggest the deployment of a covert missile, whose usage the Pentagon has never verified but which is thought to have been engaged in past targeted killings of terrorist leaders. The employment of *"Hellfire missiles"* – especially, the Hellfire AGM-114 – was mentioned by US officials. These missiles are notorious for their intense explosions and the collateral damage they frequently cause. According to the evidence left behind during the American strike on Ayman Al-Zawahiri's home, the CIA employed the Hellfire R9X, a different kind of missile derived from the AGM-114. Developed during the Obama administration, the R9X, sometimes referred to as the *"ninja bomb"* is alleged to be devoid of an explosive charge. Its six blades shred its target without causing an explosion effect since they deploy before impact (Ib.).

CONCLUSION

Extremely effective actions and operations require planning that involves full-spectrum warfare, covering a wide range of instruments coming from conventional warfare, nuclear instruments, and hybrid warfare, including informational and cognitive realms, but also civilian means that could not fit into warfare definition. Integrating and planning such actions in one central command and control point and combining with surprise and unconventional means add to the original effect. We avoid, on purpose, limiting in any way, by trying to make a list of the military and non-military means, or to define just a number of integrated instruments to be used in full-spectrum warfare. Imagination, unknown unknowns, and thinking the unthinkable are vivid proofs that the instruments integrated are limitless.

Extremely effective actions and operations require planning that involves full-spectrum warfare, covering a wide range of instruments coming from conventional warfare, nuclear instruments, and hybrid warfare, including informational and cognitive realms, but also civilian means that could not fit into warfare definition.

REFERENCES:

1. Abdyraeva, C. (2020). *"Hybrid Warfare: Trends, Challenges and Means"*, in *The Use of Cyberspace in the Context of Hybrid Warfare. Means, Challenges and Trends,* OIIP – Austrian Institute for International Affairs, https://www.jstor.org/stable/resrep25102.6., retrieved on 2 May 2025.
2. Alston, P. (28 May 2010). '*Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions. Addendum: Study on Targeted Killings'* (A/HRC/14/24/Add.6), Human Rights Council, United Nations General Assembly, para. 46.
3. Hearings on 24-25 June 1981, Commission for Science and Technology of the US Congress, https://books.google.be/books?id=dRMrAAAAMAAJ&pg=PA73&dq=%22unknown+unknowns%22&hl=en&sa=X&ved=0ahUKEwjhnraJ-7XmAhVGi1wKHUi0Bl0Q6AEIKTAA#v=onepage&q=%22unknown%20unknowns%22&f=false, retrieved on 21 May 2025.
4. Aviation Week and Space Technology (29 July 1974), 57.
5. Ball, D., Waters, G. (2013). *Cyber Defence and Warfare*, Security Challenges, vol. 9, nr. 2. The 2013 Defence White Paper (2013), pp. 91-98, Institute for Regional Security, https://www.jstor.org/stable/26462919, retrieved on 21 May 2025.
6. BBC (7 December 2020). *Mohsen Fakhrizadeh: 'Machine-gun with AI' used to kill Iran scientist*, https://www.bbc.com/news/world-middle-east-55214359, retrieved on 3 May 2025.
7. Berg, R. (23 December 2024). *Ex-Israeli agents reveal how pager attacks were carried out*, BBC, https://www.bbc.com/news/articles/cwy3l02wxqdo, retrieved on 21 May 2025.

8. Brooks, R. (2016). *How Everything Became War and the Military Became Everything: Tales from the Pentagon*. New York: Simon & Schuster.
9. MG Chiarelli, P. W., U.S. Army, MAJ. Michaelis, P.R. (July-August 2005). U.S. Army, *Winning the Peace. The Requirement for Full-Spectrum Operations*, in *Military Review*, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/COIN-Reader-1/Chiarelli-JA-2005/, retrieved on 2 June 2025.
10. Chifu, I. (July 2025). *Conceptualizare și evaluare epistemologică. Războiul cognitiv/Conceptualization and epistemological evaluation: Cognitive warfare*, in *Infosfera*.
11. Chifu, I., Simons, G. (2023). *Rethinking warfare in the 21st Century. The influence and effects of the Politics, Information and Communication Mix*. Cambridge University Press.
12. Chifu, I. (2022). *Studii prospective și metodologii alternative. Eșafodajul de securitate în secolul 21/Prospective studies and alternative methodologies. Security Establishment in the 21st Century*. București: Editura RAO, vol. 3 – Reshaping Global Security and International Relations in the 21st Century/Reconfigurarea securității și a Relațiilor Internaționale în Secolul 21 (The Tetralogy hereafter).
13. Clark, I. (2015). *Waging War: A New Philosophical Introduction*, 2nd ed., Oxford: Oxford University Press, p. 79.
14. Commonwealth of Australia, *Defence White Paper 2013.* Canberra: Department of Defence, para 3.9.
15. Courtney, H., Kirkland, J., Viguerie, P. (1997). *Managing uncertainty, Strategy Under Uncertainty*, Harvard Business Review, November-December, https://hbr.org/1997/11/strategy-under-uncertainty, retrieved on 2 June 2025.
16. *Defence White Paper 2013*, pp. 29-30, and Vice Admiral Ray Griggs, Chief of Navy, *"The Navy's Role in the Maritime Century"* (speech, Lowy Institute for International Policy, Sydney, 17 August 2012), http://www.lowyinstitute.org/files/griggs_-_the_navy_in_the_maritime_century.pdf., retrieved on 2 May 2025.
17. *Defending Australia in the Asia Pacific Century: Force 2030*, p. 27.
18. Department of Defence (2000). *Defence 2000: Our Future Defence Force*. Canberra: Defence Publishing Service, p. 23.
19. Department of Defence (2013). *Defence White Paper 2013: Defending Australia and its National Interests*. Canberra: Commonwealth of Australia, p. 30.
20. Department of Defence (2009). *Defending Australia in the Asia Pacific Century: Force 2030.* Canberra: Commonwealth of Australia, p. 49.
21. DoD News Briefing – Secretary Rumsfeld and Gen. Myers, Presenter: Secretary of Defense Donald H. Rumsfeld, 12 February 2002, https://archive.defense.gov/Transcripts/Transcript.aspx?TranscriptID=2636, retrieved on 21 May 2025.

22. Donnelly, C., director, Institute for Statecraft. War in Peacetime. Coping With Today's Changing World, file:///C:/Users/Iulian/Downloads/71-74_CHRIS%20DONNELLY_ANG.pdf.
23. Dupont, A. (2015). *Full spectrum defence: Re-thinking the fundamentals of Australian defence strategy*, Lowy Institute for International Policy http://www.jstor.com/stable/resrep10131, retrieved on 12 May 2025.
24. Enemark, C. (2023). *Moralities of Drone Violence,* Chapter WARFARE, Edinburgh University Press, https://www.jstor.org/stable/10.3366/jj.7358669.6, retrieved on 22 May 2025.
25. *Ex-top manager of fugitive oligarch Kurchenko's firm detained in Greece upon Ukrainian request*, UNIAN Information Agency, 3 March 2019, retrieved on 13 May 2025.
26. Favier, S. (3 August 2022). *Ayman al-Zawahiri's death: What is the Hellfire R9X missile that the Americans purportedly used?,* Le Monde: https://www.lemonde.fr/en/international/article/2022/08/03/ayman-al-zawahiri-s-death-what-is-the-hellfire-r9x-missile-that-the-americans-purportedly-used_5992310_4.html, retrieved on 22 May 2025.
27. Fowler, M. (2014). *The Strategy of Drone Warfare*, in *Journal of Strategic Security*, vol. 7, no. 4, Special Issue: Future Challenges in Drone Geopolitics (Winter), pp. 108-119, University of South Florida Board of Trustees, https://www.jstor.org/stable/10.2307/26465233, retrieved on 22 May 2025.
28. Gowing N., Langdon, C. (2015). *Thinking the Unthinkable, a new imperative for leadership in the digital age*, interim report for the Churchill 2015, 21st century Statesmanship Global Leaders Programme, https://www.slideshare.net/nudripakke/pdf-download-thinking-the-unthinkable-a-new-imperative-for-leadership-in-the-digital-age-pdf-free, retrieved on 21 May 2025.
29. Gozzi, L. (2 June 2025). *How Ukraine carried out daring 'Spider Web' attack on Russian bombers*, BBC: https://www.bbc.com/news/articles/cq69qnvj6nlo, retrieved on 14 May 2025.
30. Greg, S., Chifu, I. (2017). *The Changing Face of Warfare in the 21st Century*, Routledge, London and New York.
31. Haidamous, S., Chamaa, M.E., Fahim, K., Chason, R. & Nakashima, E. (17 September 2024). *Thousands injured in Lebanon as pagers used by Hezbollah explode*, The Washington Post: https://www.washingtonpost.com/national-security/2024/09/17/lebanon-pagers-exploding-hezbollah/, retrieved on 21 May 2025.
32. Halper, S. (ed.) (May 2013). *"China: The Three Warfares"* Report for the Director of Office of Net Assessment, DoD.
33. Hambling, D. (30 November 2020). *Why A Remote-Controlled Machine Gun Was The Perfect Weapon For Assassinating Iranian Nuclear Scientist*, Forbes, retrieved on 21 May 2025.

34. Hellyer, M. (2020). *From concentrated vulnerability to distributed lethality – or how to get more maritime bang for the buck with our offshore patrol vessels*, in THE CONCEPT OF OPERATIONS, Australian Strategic Policy Institute, https://www.jstor.org/stable/resrep25135.8, retrieved on 21 May 2025.
35. Herman, K. (1985). *Thinking the unthinkable in the 1980's*, Touchstone.
36. Herrmann, R.K. (2017). *How Attachments to the Nation Shape Beliefs About the World: A Theory of Motivated Reasoning,* in International Organization, vol. 71.
37. Hoffman, M. (2007). *Academic's Dictionary of Mass Communication*. Academic (India) Publishers, New Delhi.
38. *In Greece, the Russian detainee Kalinin was released at the request of Ukraine*, Teller Report, 7 March 2019, http://www.tellerreport.com/news/--in-greece--the-russian-detainee-kalinin-was-released-at-the-request-of-ukraine-.S1bpqMr0IE.html, retrieved on 21 May 2025.
39. Joint Chiefs of Staff (March 2004), *National Military Strategy*, March 2004, p. 23.
40. Jonsson, O., Seely, R. (2015). *Russian Full-Spectrum Conflict: An Appraisal After Ukraine*, in *The Journal of Slavic Military Studies*, nr. 28:1, 1-22, DOI: 10.1080/13518046.2015.998118.
41. Lindsay, J.R. (2013). Stuxnet and the Limits of Cyber Warfare. Security Studies, 22(3).
42. Logan, D.C. (2009). *Known knowns, known unknowns, unknown unknowns and the propagation of scientific enquiry*, in *Journal of Experimental Botany*, vol. 60, nr. 3, https://doi.org/10.1093/jxb/erp043, retrieved on 22 May 2025.
43. Mazhulin, A., Holmes, O., Swan, L., Boulinier, L.&Hecimovic, A. (2 June 2025). *Operation Spiderweb: a visual guide to Ukraine's destruction of Russian aircraft*, The Guardian, https://www.theguardian.com/world/2025/jun/02/operation-spiderweb-visual-guide-ukraine-drone-attack-russian-aircraft, retrieved on 22 May 2025.
44. Michalopoulos, S. (10 August 2018). *Russian meddling in Greek domestic affairs 'unacceptable,' Commission says*, Euractiv, https://www.euractiv.com/section/global-europe/news/russian-meddling-in-greek-domestic-affairs-unacceptable-commission-says/, retrieved on 22 May 2025.
45. Norberg, J., Westerlund, F., Franke, U. (2014). *'The Crimea Operation: Implications for Future Russian Military Interventions'*, in N. Granholm, J. Malminen, and G. Persson (eds.*), A Rude Awakening: Ramifications of Russian Aggression towards Ukraine*, Swedish Defence Research Agency, Stockholm, pp. 41, 48.

46. Pape, R. (1996). *Bombing to Win: Air Power and Coercion in War*, Cornell: Cornell University Press.
47. Parlin, K., Riihonen, T., Le Nir, V., Bowyer, M., Ranstrom, T., Axell, E., Asp, B., Ulman, R., Tschauner, M., Adrat, M. (August 2021). *Full-Duplex Tactical Information and Electronic Warfare Systems*, IEEE Communications Magazine, vol. 59, no. 8.
48. Plummer, R., Murphy, M. (2 August 2022). *Ayman al-Zawahiri: Al-Qaeda leader killed in US drone strike*, BBC, https://www.bbc.com/news/world-asia-62387167, retrieved on 21 May 2025.
49. Pomerantsev, P., Weiss, M., *The Menace of Unreality. How The Kremlin Weaponizes Information, Culture and Money*, Institute of Modern Russia, The Interpreter, retrieved on 21 May 2025.
50. Reichborn-Kjennerud, E., Cullen, P. (2016). *What is Hybrid Warfare?*, Norwegian Institute for International Affairs (NUPI), http://www.jstor.com/stable/resrep07978, retrieved on 12 May 2025.
51. Rumsfeld, D., Guidance and Terms of Reference for the 2001 Quadrennial Defense Review, 22 June 2001, http://www.comw.org/qdr/qdrguidance.pdf, 7, retrieved on 11 May 2025.
52. *Russian businessman wanted by Ukraine freed, lawyer says*, ekatmimerini.com, 7 March 2013, http://www.ekathimerini.com/238390/article/ekathimerini/news/russian-businessman-wanted-by-ukraine-freed-lawyer-says, retrieved on 21 May 2025.
53. Ryan, M., *"Full spectrum dominance": Donald Rumsfeld, the Department of Defense, and US Irregular Warfare Strategy, 2001-08*, University of Nottingham, research repository, at https://nottingham-repository.worktribe.com/output/728132/full-spectrum-dominance-donald-rumsfeld-the-department-of-defense-and-us-irregular-warfare-strategy-2001-2008; *Quadrennial Defense Review*, Section 3, retrieved on 21 May 2025.
54. Seddon, M. (2 June 2014). *'Documents Show How Russia's Troll Army Hit America'*, Buzz Feed, Documents Show How Russia's Troll Army Hit America.
55. Shaw, I.G.R. (2016). *Predator Empire. Drone warfare and full spectrum dominance*, University of Minnesota Press, Minneapolis and London.
56. Simons, G., Chifu, I. (2025). *Information Warfare as a Theoretical Construct and an Operational Practice*, in Samoilenko, Serghei&Solon, Simmons, *The Handbook of Social and Political Conflict*.
57. Slessor, J.C. (1936). Air Power and Armies, London: Oxford University Press.
58. Taleb, N.N. (2010). *The Black Swan. The Impact of the Highly Improbable,* Random House.
59. Trung Anh, D. (2002). *Known Knowns, Unknown Knowns, and Unknown Unknowns What you know and what you don't?*, Data Driven Investor, https://medium.com/datadriveninvestor/known-knowns-unknown-knowns-and-unknown-unknowns-b35013fb350d, retrieved on 22 May 2025.
60. Walpole, N.J.R. (2012). *Thinking the Unthinkable: The Lives of Royal Air Force and East German Fast-Jet Pilots in the Cold War*, Astonbridge Publishing, ISBN 9780953793327, 250 p.
61. Warden III, J.A. (1995). *"The Enemy as a System"*, in *Airpower Journal* (Spring), pp. 40-55.
62. Weil, K. (2010). *Measuring Tweets*, https://blog.twitter.com/2010/measuring-tweets, retrieved on 21 May 2025.
63. Zâgar, M. (2017). *Toți oamenii Kremlinului. O scurtă istorie a Rusiei Contemporane*, Cartier, ISBN 978-9975-86-210-3, 415 p.
64. https://onlinelibrary.wiley.com/doi/10.1002/9781119895534.ch29, retrieved on 21 May 2025.
65. https://www.thinkunthink.org/, retrieved on 21 May 2025.