Hybridity: New Threats, Strategic Shift?

Jerome Clech

PhD, PSD R3C - ESD R3C CNAM PARIS

Abstract

In a context won by hybridity, the question is to know what "grand strategy" can effectively manage the unexpected and reduce friction in order to achieve a "culmination of success", to use Clausewitz's words, in a world plunged into the era of asymmetric conflicts—even though the occurrence of state-to-state conflicts remains to be considered.

Keywords: Hybrids, Terror, Threats, Friction, Conflict

Hibridez: ¿nuevas amenazas, cambio estratégico?

Resumen

En un contexto ganado por la hibridación, la cuestión es saber qué "gran estrategia" puede gestionar eficazmente lo inesperado y reducir la fricción para lograr una "culminación del éxito", para usar las palabras de Clausewitz, en un mundo sumergido en la era de la asimétrica Conflictos, a pesar de que queda por considerar la ocurrencia de conflictos entre estados.

Palabras clave: Híbridos, Terror, Amenazas, Fricción, Conflicto

混杂性：新威胁和战略转变？

摘要

在充满混杂性的情境下，问题在于了解什么样的“大战略”能有效控制意外事件并减少摩擦，进而实现“大获全胜”，按学者Clausewitz的话来讲，在一个充满非对称冲突的时代，甚至国与国之间的冲突都有待衡量。

关键词：混杂，恐怖，威胁，摩擦，冲突

doi: 10.18278/ijc.8.2.5

The phenomenon of friction, which consists of an inevitable gap between a strategy and its implementation, was theorized by Clausewitz. It is even more true today because the world is apolar, according to R. Haass: the international context is blurred and shifting. Indeed, since the end of the Cold War, the growing interconnection of a multitude of disparate actors with diverse loyalties is at the origin of a "full" world for G. Duby, fragmented, and with an increased conflictuality. But this conflictuality, due to fracture lines that are sources of instability and uncertainty, no longer responds to a Hobbesian logic: confrontations between States which were frank, brutal and rather well circumscribed have been replaced by ill-defined crises, even undefined in all their dimensions: unfolding in “grey-zones”, those regions neither at war nor at peace, they involve polymorphous actors, neither warriors, nor criminals, nor traffickers, nor ideologues, but all of these at once, and sometimes even more so, who resort to diverse modes of action, both symmetrical and asymmetrical. Without being fundamentally new, hybridity is today an inescapable phenomenon because it characterizes most contemporary conflicts. As M. Naïm, editor of *Foreign Policy* magazine, points out in his book *Illicit*, the analyst's tendency to classify, arrange and categorize once and for all misses the hybridization of threats. As a result, the answer provided are no longer necessarily adapted. Consequently, some people do not hesitate to question the usefulness of military power in terms of "grand strategy", denouncing its bankruptcy, following the example of M. Van Creveld. They even go so far as to wonder whether war is not “obsolete”, to use J. Mueller’s words. However, if the exclusive use of *hard power* shows its limits (case of the ^{2nd} Gulf War), it would be illusory to rely solely on *soft power*: commercial and financial coercion measures are not always more effective (example of the Helms-Burton law against the Castro regime).

In a context won by hybridity, the question is to know what “grand strategy” can effectively manage the unexpected and reduce friction in order to achieve a “culmination of success”, to use Clausewitz's words, in a world plunged into the era of asymmetric conflicts—even though the occurrence of state-to-state conflicts remains to be considered.

The hybrid threats responsible for staggering unforeseen events must be met with an innovative hybrid strategy, capable of minimizing the friction and leading to political success.

Hybridity has become a key concept because the phenomenon of asymmetry is taking on an unprecedented scope today. Talking about hybrid threats means capturing reality accurately and providing a useful conceptual framework to think about new realistic and operational strategies.

The rise of the hybrid threat

Associated with asymmetric warfare, the phenomenon of hybridity is now taking on an unprecedented scope.

Hybridity is not a new reality: it is as old as asymmetric combat

In his book *La guerre asymétrique et l'avenir de l'Occident* (2003), S. Metz provides a particularly detailed analysis of the phenomenon of strategic asymmetry, which allows him to characterize it in detail: "dimensions of strategic asymmetry"; "levels of asymmetry"; "forms of asymmetry". Asymmetry has many dimensions. For example, it can be "positive" or "negative", depending on whether it consists of "maintaining and enhancing an existing superiority" (in the case of the United States, where the emphasis is on training, command and technology) or "exploiting an opponent's weakness " (public opinion in democracies). It can be "low risk" (the case of propaganda) or "high risk" (terrorism).

Asymmetry commonly concerns the "operational" level (as in the case of the use of submarines by the Germans against surface ships during the Second World War), but also the "strategic-military" level (the famous concept of "massive reprisals"), or the "political-strategic" level when it comes to obtaining a military advantage with non-military means (projection of a victim image on the international scene, following the example of Slobodan Milosevic or Saddam Hussein).

Asymmetry can take several forms. Asymmetry of "method" refers to the use of operational concepts and doctrines different from the opponent's (the case of guerrilla warfare and non-linear operations in general). Asymmetry of "will" refers to the situation where one side protects its vital interests, while the other protects strategic or power interests; it is linked to "normative" asymmetry, a situation in which the actors have different value frames of reference, the use of kamikaze attacks being an illustration of this (facing death is part of the strategy) The asymmetry of "organization" allows an advantage over the classic hierarchical model (case of clandestine insurgent networks). Finally, the asymmetry of "patience" refers to a temporality relative to the actor (the United States favors short conflict resolutions, whereas the Eastern conception of time supports the effectiveness of long conflicts).

Theorizing about asymmetry provides keys to understanding current hybrid wars, in their asymmetric aspects.

The erosion of borders of all kinds has consecrated hybridity, whose reality is enriched and complexified

A neo-realist reading of international relations, based on the relationship of powers, shows the existence of a correlation between the balance of powers and the development of asymmetric warfare. Indeed, during the Cold War, the nuclear weapon and the existence of NATO limited the risks of direct confrontation between the two blocs. Therefore, the world saw an increase in asymmetrical conflict, because the strategic value of this type of conflict was high. According to a unipolar vision of the world after 1991—at least in military terms—dear to S. Huntington in particular, the end of the Cold War having further minimized the risk of inter-state confrontations, asymmetric conflicts have become predominant. And hybrid warfare has also become de facto, because armed non-state organizations cannot confine themselves to classical military action, the military superiority of Western states being undeniable, particularly that of the United States (notably through the RMA—*Revolution in Military Affairs*).

Globalization has not put an end to the dissymmetry of *hard power* between developed states and non-state actors, but it is an equalizer of power in almost all areas of *soft power* (culture, influence, media, social networks, propaganda, etc.), intimately linked to the informational sphere or "infosphere". For all of them, information moves at the speed of light[1]—or almost. By investing in the infosphere (propaganda, attacks on information and communication systems, attacks with a high media impact, etc.), non-state actors have been able to take advantage of the opportunities offered by the infosphere. Non-state actors have restored the symmetrical aspect of the confrontation, but in a practically non-kinetic register. From then on, the hybridity of war took a new turn: where it used to consist of a limited symmetrical component and a predominantly asymmetric component, essentially kinetic, it now consists of an asymmetric kinetic component that remains - despite everything - minor, but that is multiplied by the efficiency of the non-kinetic symmetrical component. As a matter of fact, terrorist attacks have an impact far greater than the number of deaths they cause, which terrorist propaganda exploits by emphasizing in its magazines (*Inspire, Dabiq*) that a few suicide bombers can shake an entire country.

Thus, hybridity is characterized less by the mere articulation of symmetrical and asymmetrical modes of action than by their capacity to enter into systemic resonance. In this respect, the nature of the actors and the space-time of the conflict are two determining factors. United Nations Security Council Resolution 1373, dated 28 September 2001, already mentioned the proximity between "international terrorism, drug trafficking, money laundering, arms trafficking, clandestine nuclear, chemical or biological substances". The use of criminal money, once laundered, is a powerful source of "legal" financing for terrorism. Hence the hybridization of activities: trade, crime and terrorism are increasingly intertwined, creating confusion for the authorities. At first glance, one might think that failed states or proto-states are solely responsible for the emergence of these hybrids. In fact, what they have in common today is that they are socio-economic actors driven by a deterritorialized ideology, like radical Islamism and *jihadism*. Moreover, as O. Roy formulates it, yesterday "radical Islamism", today "islamized radicals". And these radicals are likely to be born everywhere, from exclusion or from a form of

[1] In fact, what is decisive is that information is in a sense faster than man; it is understandable that the information society has been refined with the Internet, but it finally began with the invention of the Chappe telegraph in 1794.

perceived failure, from a combination of personal factors that escape all analytical grids. The suicide bombers of the Islamic State (IS) or the Boston terrorists are edifying illustrations of this. Finally, increasing the degree of complexity, meta-hybrids are born from hybrid alliances that are formed in reaction to localized measures: this is how the *Patriot Act*, by rightly targeting the financing of terrorism, has indirectly complicated the investments of Colombian cartels in the United States, which have subsequently joined forces with the *Ndrangheta* (Calabrian mafia) to launder the proceeds of drug trafficking, via Europe. Reinforcing each other, these mafias strengthen at the same time drug trafficking, and at the end of the chain, international terrorism, which feeds largely on it (as in Afghanistan, where a farmer can be a farmer, a drug trafficker, a Taliban and a terrorist at the same time).

To hybrid threat, hybrid strategy

Hybridity is a useful concept for defining innovative and adapted defense and security strategies.

The deficiencies of national defense and security strategies regarding hybrid threats

In France, if the five strategic functions defined by the 2013 Livre Blanc, then by the successive Strategic Reviews (2017 and 2020) which remain relevant, "intervention", when it includes the dispatch of an expeditionary force, by the cost (human and budgetary) that it implies, can only be used sparingly, which shifts the burden to other strategic functions. However, "deterrence" can only respond to attacks on vital interests by a state actor, which is not the case of hybrid threats (e.g. the Islamic State, despite the name). Moreover, it is illusory to believe that "knowledge/anticipation" can systematically "nip in the bud" the prodromes of a future attack/conflict; as for "protection", it is, like any "shield", necessary but not sufficient, the "sword" always triumphing in the end. A strategic gap then appears.

At the same time, the term "military tool" is increasingly used because military victory, when there is an intervention, is less than ever decisive. "Influence" consists in particular in "winning hearts and minds", according to the expression introduced by J. de Nye: this is the whole issue of the "global approach" and post-conflict reconstruction (public order, justice, political, economic and social development, democracy assistance). However, Kant already announced the limits of democratization. But this observation does not exempt the international community from getting involved in the reconstruction of a failed state, which is always a source of unforeseen strategic problems due to the weakness of the existing government, as was the case in Iraq. Yet, the Afghan theater has clearly shown the limits of this approach.

"Augmented prevention"[2], on sensitive points: hybrid strikes, stealthy or regular?

Mechanically, the will to push back the threshold for large-scale military engagement in the event of asymmetric attacks thus creates a gap that could be filled by the use of a form of "augmented prevention": current prevention would be extended to in-depth action aimed at intimidation and early disruption: Cyber offensive, not only in the physical part of cyberspace, but also in the logical and socio-cognitive dimension of cyberspace, i.e. the infosphere; remote strikes (cruise missiles, armed drones in particular); raids (special operations, clandestine operations) directed against an identified adversary, which could go as far as destroying its material or non-material sensitive points, by powerful and precise actions with limited collateral effects, without necessarily communicating about it (as illustrated by President B. Obama's "stealth strategy"). Of course, these are only processes, but Beaufre has already emphasized the importance of the "choice of processes" to give substance to a strategy.

Thus defined, the strategic function of augmented prevention is based on strategic principles that can be identified by the "synthetic method" theorized by Castex: the principle of concentration/extension of forces (use of force on centers of gravity: head of hybrid networks, headquarters, support of the local population) and principle of activity or direction (parallel use of available means); principle of initiative (early intervention, even preventive); principle of surprise on centers of gravity (treatment of High Value Targets—HVT—by drone, *Stuxnet-type* viruses on the information and communication systems of the essential infrastructures, special or clandestine operations for obstruction) ; principle of freedom of action (the offensive character of augmented prevention would balance the defensive character of operation "Sentinel", in order to indirectly reinforce the protection of the national territory); principles of saving forces and security (remote strikes preserve the combatant); principle of maneuver (ends in line with means: delaying or even preventing the outbreak of a large-scale conflict using a strategic function at the interface of deterrence and intervention).

Effective because of their hybrid nature, remote strikes are thus made possible by technology, which is also the source of ethical developments. This is the case of armed drones, and in the future, of combat drones. Capable of striking high-value human targets without involving combatants, they constitute a hybrid mode of physical action: a military response, though largely dehumanized. The

[2] Term introduced in the context of work related to the Livre Blanc on Defense and National Security (2013). It refers to the "augmented human being", whose natural capacities are increased by technologies at the origin of paradigm shifts: yesterday, new information and communication technologies; today, their material extension (artificial intelligence and the Internet of Things, 3D printing); tomorrow, the convergence of NBIC (nanotechnologies, biotechnologies, information and cognitive technologies).

war waged by the CIA with the help of armed drones from its headquarters against the heads of terrorist networks in Pakistan, Syria, Somalia, in the Sahel-Saharan strip and elsewhere, illustrates this originality of a combatant absent from the theater (operating from his garrison, for example), whose daily life is also hybrid: between stealth warfare and family serenity. Acting in a complementary manner, special operations also constitute, in their own way, remote strikes. Because their action on the ground, between missions of advice and training of a third-party armed force and indirect intervention, proceeds from reduced manpower projected in depth but with an effect multiplied by the *proxies* in play.

Capable of neutralizing an "intelligent core", cyber offensives constitute a hybrid mode of action: for material purposes when it comes to hitting the physical dimension of cyber space; for immaterial ones when it comes to exploiting or reaching the infosphere. Active Cyber Defense (ACD), hybrid by nature in that it involves internalizing *hacking* skills within the defense, is cyber offensive mode acting on the logical part, and the one that immediately comes to mind. But reducing cyber offensives to ACD would be a mistake. Indeed, thanks to the ubiquity and length of the air arm, an explosive or, one day, electromagnetic bomb can act on the physical dimension and neutralize a *Command and Control* center. Moreover, Electronic Warfare (EW), by exploiting the continuity of the aerospace environment, already allows the acquisition of a significant part of the technical intelligence that is useful in particular for counter-terrorism. Finally, through "coercive diplomacy", a term coined by P. Venesson, the air power is able to act on the socio-cognitive dimension, by influencing the field of perceptions and representations of the adversary, and can thus intimidate him in the end: either by the *show of force* or the potential use of leaflet bombs, opponents' moral can thus be undermined.

"What matters is what works", said T. Blair. If remote strikes come with the redefinition of the ethical framework driven by the acceleration of technological progress, international law still does not take note of it: aggression can only be characterized when the supposed perpetrator is a State, and the use of force, under Chapter 7 of the United Nations Charter or within the framework of self-defense (Art. 51), applies only to a State. As a result, the Security Council resolutions relating to the fight against terrorism (as in the case of the intervention in Afghanistan in 2001) are out of step with the charter itself; resolution R2249 authorizing the intervention against *Daech* confirms this gap in international law, by being compelled to recognize the "exceptional" nature of the threat. Of course, augmented prevention assumes its share of ambiguity and stealth, but its legitimacy in practice would be reinforced by an amendment to the charter moving toward the recognition of transnational threats, and hybrid threats more generally.

“Augmented prevention", on flows and through networks: from hybrid border surveillance to a renewed global approach

Bringing added value in terms of observation, drones are used in the civilian domain for border surveillance in the United States. The aim is not only to hinder illegal immigration, which is known to irrigate the entire spectrum of the illegal economy, bur also to illegal trafficking (arms, drugs, counterfeit goods, etc.), which hybridizes the threats and provides a breeding ground for international terrorism. The use of drones could reinforce the Frontex[3] system at the borders of the European Union (EU), or the control of national borders, particularly in time of state of emergency. Of course, the effectiveness of the system would depend on its level of integration into the range of sensors operated by the intelligence community (DGSE, DGSI, DNRED, TRACFIN, DRM and DRSD).

From border control to border risk management, the emergence of the concept of "*smart borders",* developed by W. Pool and G. Passantino, corresponds to the implementation at airports of "intelligent" combinations based initially on biometrics. The aim is to characterize and identify the potential threat posed by an individual according to his or her behavioral profile. For example, the PNR (*Personal Name Record*) is a device[4] for assessing the risk that a traveler is linked to a terrorist enterprise. It is designed to know "what the individual has done" before booking a flight and to predict, "what he or she is likely to do" at destination. The EU sees these biometric developments as useful for managing risk at the border, but they can also—and more importantly—be used to track the threat and gather intelligence to hinder it in time. This implies that the EU requires GDSs[5] (*Global Distribution Systems*) to share information that may be of interest in the fight against terrorism with national intelligence agencies, but also implies that the intelligence community should make an effort to ensure greater fluidity in information flow within it. As a predictive tool for decision support, PNR is subject to a margin of uncertainty and error. In order to reduce this error while refining the tracking of individuals linked to a terrorist enterprise, the hybrids, *datamining*[6] must focus on the main domains that they cross: cyber activities (especially on the Web), more or less legal economic activities and financial flows—even and especially of small amounts, terrorism being a cheap mode of action. In order to see more clearly into the digital maze generated by the "computerization of the body"[7] and of human activities, it could then be useful to cross-reference the PNR with the files held

[3] European Border and Coast Guard Agency.

[4] Adopted by the United States, Canada, Australia and the United Kingdom, this system will also apply to the EU.

[5] Electronic platforms for managing airline reservations, at the interface between travel agencies, airlines and travelers, like Amadeus created by Air France, Iberia and Lufthansa.

[6] Exploitation and analysis of databases using algorithms.

[7] Concept of *shadow body,* developed by I. Van der Ploeg.

by national defense and security forces, and more particularly those held by the agencies of the intelligence community.

It is all about minimizing the risk at the border by filtering profiles and behaviors that could constitute a threat. But it is also a question of gathering information to prevent crime at the source, notably outside our borders. To this end, when a footprint on the ground is indispensable (without going as far as massive intervention), civil-military synergies are necessary. Instead of the compartmentalized juxtaposition of various means that characterizes the "global approach" implemented in Afghanistan, we need to replace it with a true systemic, synchronized and centralized operation. According to H. Coutau-Bégarie: "In contemporary times, the strategist is no longer the one who leads armies, but the one who coordinates and makes forces of different kinds act: military, economic (total war), political (ideological confrontations, support from third countries), and social (influence on the populations). The key is human interoperability. This requires the construction—upstream—of networks (network-to-network warfare, as advocated by D. Petraeüs): civil-military networks, for example by opening the Ecole de Guerre to civilian executives (which is partially done today) from sectors related to defense and security, in particular development actors (NGOs, industrialists present on the territory of theaters, investors); friend-enemy networks, by de-dramatizing negotiations with the enemy and the necessary concessions, as well as the "recycling" of former enemy combatants into intelligence or psychological action[8] units present on the concerned territory. Finally, putting as much pressure as possible on entities involved in critical "triangular" relationships (in the case of the fight against the EI, which is far from over: Turkey vis-à-vis Kurds and the United States, or Saudi Arabia vis-à-vis Iran and the United States) could encourage them not only to limit their discreet support for hybrid threats, but also to facilitate the peace operations that a multinational coalition would have to carry out in the event of an intensification of the engagement.

Conclusion

In short, if the gap between planning and conducting a strategy is not new in strategic thinking, the era of hybrid threats reveals a lack in the spectrum covered by the strategic functions of national defense and security policies, causing unfore-

[8] "At the bottom of Alexander's victories, we always find Aristotle," said General de Gaulle. In other words, there are two dimensions to strategy: one material, the other intellectual. The philosophical, psychological (Beaufre) and rhetorical dimensions also remain essential (the RMA, for example, has shown its limits). J. Baud believes that the root cause of Islamist terrorism results more from a series of dichotomies on a global scale (integration/differentiation; modernity/tradition; technology/spirituality; moral values/economic values), thus illustrating the "clash of civilizations" theorized by S. Huntington. Following the logic of J. Baud, it would be necessary to put human intelligence at the forefront in order to understand and manipulate the "mental universe" of the enemy. Whether one agrees with the diagnosis or not, the conclusion remains interesting.

seen events that are difficult to manage[9], which augmented prevention could fill, provided that the necessary equipment and capabilities are available.

Offering the decision-maker a wider margin of strategic maneuver, at the crossroads of surveillance, control, intimidation and "strategic coercion" (R. Pape), it could be extended by a war of manipulation through a renewal of the global approach, aiming not only—as far as possible—at the development of the territory concerned, but also and above all at the collection of actionable intelligence for the benefit of risk management at the borders, of useful targeting for long-distance strikes or of hindrance through commando actions. International law, which is partly unsuited to the new face of conflicts, could change in order to take into account the frequently transnational and hybrid nature of threats, and thus offer a priori legal legitimacy to hybrid strategies and procedures that are needed to combat them.

Beyond that, the continuum of security between internal and external affairs, reaffirmed by the French "grand strategies", makes it necessary to ask the question of the articulation between augmented prevention and protection. Indeed, the culturalist and religious rhetoric often preferred by hybrids in the last two decades should not hide the reality of their rootedness in national territories: exploitation of economic, social and security weaknesses in certain urban or peri-urban areas that have sometimes become lawless zones. If defense in France can play a major role in reinforcing the spirit of citizenship according to modalities to be defined, closer interdepartmental coordination between defense, police, justice, national education and economic development could be considered.

Bibliography

Albertsen (2003), "The Paradigma Web Harvesting Environment", *3rd ECDL Workshop on Web Archives*, Trondheim, Norway.

Bacevitch (2010), *Washington Rules: American path to the permanent war*, Metropolitan Books, Henry Holt and Company, New York.

Badie (2004) *L'impuissance de la puissance. Essai sur les nouvelles relations internationales*, Paris, Fayard.

Baud (2003) *La guerre asymétrique ou la défaite du vainqueur*, Monaco, Editions du Rocher, Pp.83-106.

[9] Among other things, for the record: observation drones, armed, but above all combat drones; cyberoffensive capacity extended to influence; cross-referencing of files and sharing of intelligence between agencies, development of hybrid relational networks.

Bauer (2009), La face noire de la mondialisation, Edition CNRS.

Baldaccini (2008), "Counterterrorim and the EU Strategy for Border Security: Framing Suspects with Biometric Document and databases", *European Journal of Migration and Law*, 10, 1, p31-49.

Borgman, Furner (2002), "Scholarly Communication and Bibliometrics. Annual Review of Information Science and Technology," ed. B. Cronin. *Information Today*, Inc.

Ceyhan (2008) "Technologization of Security: Management of Uncertainty and Risk in the Age of Biometrics," *Surveillance & Society, 5(*2).

Ceyhan (2009), Antiterrorism and Technologies, *International and Strategic Review.*

Chamagne (2012), *The Art of Air Warfare*, Strategies and Defense collection, *Strategic Reflections.*

United Nations Charters (1945).

Daguzan and Lorot (2008), "Rethinking national security", *Sécurité globale.*

Debray (1989), *Tous azimuts*, Edition Odile Jacob.

Deleuze and Guattari (1987) "Rhizome", *Thousant Plateaus.*

Ehrenfeld, Rachel. *Narco-terrorism*. New York, Basic Books, 1990.

Eick (2009), *The Droning of Drones: the Increasingly Advanced Technologies of Surveillance and Control*, Statewatch.

Erickson and Haggerty (2006), "The Surveillant Assemblage,*" British Journal of Sociology*, 51(4) December: p605-622.

Europa, official Website of the EU, http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l24402_fr

FATF-GAFI (2001), official Website, http://www.fatf-gafi.org/pages/0,3417,fr_32250379_32236982_1_1_1_1_1,00.html

Feenberg (2009), "Ten Paradoxes of Technology," *Biennial meeting of the Society for Philosophy and Technology.*

Fukuyama, Francis (1989) "The End of History," *The National Interest*.

Gaddis, John (1987) *The Long Peace. Inquiries into the History of the Cold War*, New York, Oxford University Press.

Géré (2015), From asymmetric warfare to hybrid confrontations, National Defense Review.

Girard (1972), *La violence et le sacré*, Hachette, collection " Pluriel ".

Hardin (2003), "Eyes in the Skies," *Richmond Times-Dispatch*, p. F1.

Hasbrouck, E. (2007), "What's in a Passenger Name Record (PNR)? " Author's website article (retrieved from http://hasbrouck.org/articles/PNR.html)

Hobbing (2008), *Tracing Terrorists: The EU-Canada Agreement in PNR matters*, CEPS Special Report.

Huntington, Samuel P. (1993) "The Clash of Civilizations? ", *Foreign Affairs*, Vol.72, N°3, Pp.22-49.

Introna and Wood (2004), "Picturing Algorithmic Surveillance: The politic of Facial Recognition Systems," *Surveillance and Society*, 2(2/3): 177-198.

Kay (2004), *Web Harvesting*. Computerworld. http://www.computerworld.com

Latour (2005). *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford: Oxford University Press).

White Paper on Defense and National Security (2013).

Lukes (2005) "Power and the Battle for Hearts and Minds," *Millennium 33* (3): 4 77-493.

Luttwak (1987) The Logic of War and Peace, Cambridge, Belknap/Harvard University Press, Pp.7-17.

Machiavelli, *The Prince.*

Metz (2003), "Asymmetric Warfare and the Future of the West," *Foreign Policy.*

Nye (2004) *Soft Power. The means to success in World Politics*, NEW YORK, Public Affairs.

O'Neil (2005), "Complexity and Counterterrorism: Thinking about Biometrics," Studies in Conflict & Terrorism, 28: p547-566.

Petraus (2010), *Conference at Sciences Po*, covered by France 24, November 23, 2010

Poole and Passantino (2003) A Risked-based-Airport Security Policy, Reason Public Policy Institute, Policy Study No. 308.

Reid, Qin, Zhou, Lai, Sageman, Weilmann, Chen (2005), "Collecting and Analyzing the Presence of Terrorists on the Web: A Case Study of Jihad Websites," *Intelligence and Security Informatics*, vol. 3495/2005, 15-17.

Reilly, Tuchel, Simon, Palaima, Norsworthy, Myrick (2003), "Political Communications Web Archiving: Addressing Typology and Timing for Selection, Preservation and Access," *3rd ECDL Workshop on Web Archives*, Trondheim, Norway.

European Security Strategy (2003). http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/r00004_fr.htm

Sorensen (2003), *Beyond the Myth of Retreat*, Palgrave Macmillan.

The New Yorker (2010), "The Predator War: the Risks of the CIA's Covert Drone Program," November 21.

Thornton, Rod (2007) *Asymmetric Warfare. Threat and Response in the Twenty-First Century*, Cambridge, Policy Press.

United States Department of Defense (2001), *Dictionary of Military and Associated Terms,* Joint Publication 1-02, p. 557.

Van Creveld (1989), *Technology and War*, London, Macmillan.

Van der Ploeg (2007), "Genetics, Biometrics and the Information of the Body," Ann Ist Super Sanita, 43(1), pp.44-50.

Venesson (1997), *Les chevaliers de l'air*, Presse de Sciences Po.

Venesson (2000), "Bombarder ou convaincre? Air Power, Bounded Rationality, and Coercive Diplomacy in Kosovo," *Culture and Conflict*, Rationality and International Relations (vol.2)

Willis et al (2005), *Estimating terrorism Risk*, RAND Corporation MG 388.