NATIONAL SECURITY, ELECTRONIC MEDIA AND FOREIGN POLICY

[**Issue Number 75 - January 2011**](https://www.lebarmy.gov.lb/en/content/75-d)

**National security, Electronic Media and Foreign Policy**   
Prepared By: Professor Michel NEHME   
Researcher

In defining the state policy, national interest and foreign policy, the starting point is the national security. However, given the diversity of partial interests that exist within a society, many of them conflicting with each other, the tasks of reconciliation and its final expression as the nation security is the responsibility of those representing the powers within the state and those who have the government function.

This allows identifying the gap between the objectives of state and government. In those, survival, safety and welfare are the immutable aspects of state targets. They are, to give its name, objectives and broader national security. As a point of reference usually governments exercise generally what correspond to a specific national project horizons established according to the timing of governance while the state sustains the basic values of conduct.

Thus, national security and objectives defining the beginning of the policy of the state - the Great Political - and allows us to separate the permanent objectives - the state - from the strategic - inherent in a government project - in order to confront and make sense of the process of political action in its broadest sense. Policy decisions are defined behaviors and set goals and courses of action and measures taken to comply. It is clear that the determination of «national interest» cannot respond solely to a single perspective. The vision of the legal, sociological, economic or military analyst is not broad enough to incorporate all the elements of a comprehensive understanding of present reality and future scenarios.

In its implementation or in the evolution of society, there are generated flows and exchanges of information between internal and external actors involved in social dynamics. These data are quantifiable and qualitative allow access, under a methodical process, an overview of national and international reality and the real determination of objective criteria, that become permanent or strategic objectives. In this perspective is the balance of national power, the most appropriate approach when analyzing foreign policy and the state ability to take action to achieve their objectives and access to what it calls its interest and security. Security seeks to meet the vital objectives of permanence and survival of the state. This is important to emphasize, as well as to dwell on the national goals and interests and acquire a theoretical significance with a defined methodology for pragmatic validation.

There is an orthodoxy that divides the power in four fields and they could be listed as:

a. The classic political,

b. Economic,

c. Psychosocial

d. Military.

This division should not lead us to consider treatment as an inert object, forgetting that a dynamic relationship exists among them in human society. The 'fields of power' are frameworks that encompass activities consistent with each other by nature and are useful for the analysis in relation to the exercise of power and the genesis of it. In terms of uses of national development, the National Power as a view for improving material and spiritual culture of society in terms of national security must be employed as a strategic tool, e.g. in order to overcome, neutralize or reduce the antagonisms that pose threat to obtaining and maintaining permanent national objectives.

The usual method is to diagnose the political reality in the broad sense that allows you to include the set of social relations within the state, political and strategic goals, according to the national interest, strategic inventory and strategic diagnosis, interpreting international stage according to the objectives and capabilities of the various instruments available to the state for external and internal action, and, finally, the action plan. The coding of information into knowledge flows «useful and vital to the survival and security of the nation», representing the efficient implementation of the instruments of power of a State, in time and more favorable circumstances achieving their goals.

In line with the above assessment of National Security, to be surprised by the contents of the WIKILEAKS is to be either negligent of international goings on, or naively trustful of governments, or both. In terms of National security, neither can be considered a virtue. The art of «diplomacy» is not, and has never been, playing nice, open and honest, rather it is a world of wining and dining, wheeling and dealing, faux courtesies, reluctant handshakes, clandestine meetings, unofficial pull-asides, deliberately vague representations of actions and policies, hush-hush cash, and blatant lies to the media, all to further personal and national self-interest or nations national securities.

Politicians, diplomats and bureaucrats like to operate within their secret world without the annoying prying eyes of journalists or taxpayers. They use the cause of national security as their immunity. They like their journalists to be little more than stenographers to power. They like their information flow to be what they determine to be best for those who vote them in, and then pay for the existence of their office. They can authorize the roaming of your bank accounts, phone conversations and even rubbish bins, but look out if their bubble is burst.

When their privacy is breached -as it has unequivocally been by Julian Assange- then that is somehow «war» and reckless endangerment. One senior American politician is calling for Wikileaks to be labeled a terrorist organization. How deeply embarrassment seems to cut when it is reddening the faces of the powerful. As the Wikileaks trove is revealed, the question of whether its public release is morally justified is relevant. The fact is of course that once we know something we can't «not to know» it, and if we know what is really going on in the pursuit of world peace, capital dominance, territorial or political hegemony, then the lofty and not quite so flash goals are potentially in jeopardy. In the digital age it is frightening to think that the diplomats and spies and their masters really considered information that about three million people had access to would stay secret. This is the era of face-book and twitter, but it is also a time when power to act is no longer the privilege of the elite few[[1]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn1" \o ").

National reality is the source of conception of foreign policy and whose needs must be satisfied that through their action in different areas in which the state interacts with the outside. From the reality when the planning process begins to take on foreign policy objective and is, in turn, a mechanism that provides guidance about what the national needs, from which the foreign policy objectives are paths is obvious that not only govern define the statistics and determine the national interest. Other factors affecting the survival of the state beside territorial integrity and full autonomy of decisions of domestic and foreign policy are the respect of classified information and the integrity of promises and confidentiality of diplomats which is the ultimate premise of any process of foreign policy. The national interest is more than the standard by which situational factors are considered relevant and suggest a certain behavior. It is also the ultimate yardstick used to measure the success or failure of the state’s foreign policy. The concept of national security is both at the starting point and purpose of the foreign policy process, so the entire sequence of events acquires a peculiarly circular confidence.

Under the American view, national security is irreducible. Henry Kissinger argues that every State must try to reconcile what he considers fair with what he considers possible. What is considered fair depends on the internal structure of the state. It may depend on its resources, geographic position and determination and resources, determination and internal structure of other states. In these terms, the nature of national power is generated from information relevant to contending powers friendly or at odd with the interests and objectives of the concerned state. For that reason alone the State is capable of exercising a responsible and national security policy as it is also designing and implementing foreign policy, which is not detached from the general reputation of integrity.

Assange may have provided the medium, but whistle-blowing has increasingly become a means by which those who have been disempowered regain a little of their suppressed or disenfranchised entitlement. Particularly so when they start to consider or get to know that their own governments are acting illegally or immorally. It is no surprise that diplomats speak in candid language and certainly no surprise that this extends to descriptions of the bare-chested, motorbike riding Putin as an «Alpha Dog» with Medvedev playing Robin to his Batman? Who thought Merkel was anything other than cautious, Sarkozy less than authoritarian, or Berlusconi would do anything other than laugh-off descriptions of him as a lightweight. The previous sentences are not my own but that of comments taken from the website of «Pundit»

Secretary of State Hillary Clinton described Wikileaks disclosure of hundreds of thousands of classified documents as «an attack» Indeed, it was the third such attack in five months that Wikileaks has launched against the United States and its international partners. Wikileaks itself has described its struggle in military terms. Founder Julian Assange recently posted a Tweet from one of his supporters declaring: «The first serious infowar is now engaged. The field of battle is Wikileaks. You are the troops»

Like the war on terror, American officials in the state department felt they have been attacked in this new cyber war in ways they did not anticipate. Over the past decade, the U.S. government has spent billions to stop foreign adversaries from remotely penetrating its computer networks for sabotage. Instead of trying to break through these defenses, Assange pioneered a new form of cyber sabotage. He found someone who allegedly penetrated its classified systems from within, downloaded America's secrets onto a Lady Gaga CD and gave them to Assange, who then disseminated this stolen information across the world. Assange has made it clear that he intends to continue posting stolen classified information and has effectively dared the United States and the world to try and stop him. He recently announced through his lawyer that if he is arrested and now he is, he will unleash a «thermonuclear device» of completely unexpurgated government files. How can we assess national security in this context when an individual like Assange has threatened America with the cyber equivalent of thermonuclear war?

It is important to remember, state department high officials argue, that these cables and conversations are not policy. Perhaps not, but definitely were used to design a consistent spotlight on what eventually establishes itself as policy, and irritatingly for politicians, give credence to the relentless work being done by many journalists to tell it like it is. This includes the Clinton directive that diplomats collect all sorts of information on foreign leaders and UN personnel including Ban KiMoon - bank account numbers, frequent flier data, and anything else the State Department may find a use for.

In their call for Assange's head on a platter, the politicians who so openly court journalists and media organizations when it suits them for personal electoral purposes, believe the documents should not have been published. Such a self-interested and shortsighted dictum would render news as mockery. For example, journalists who cover Afghanistan's corrupt and problematic Karzai government, the billions of unaccounted for US dollars that have poured in to that country and been spirited out just as quickly, and the seriously damaging impact the war is having on neighboring Pakistan, now know for certain their conclusions are spot on, despite official cautions or outright denials. The cables reveal it all. Again where are the values behind national security that the United States has to defend?

Wikileaks has been given, and in turn passed on, a minefield of information. What is possibly new is confirmation that China is sick to death of the «spoilt child» antics of North Korea and could approve of the two Koreas being reunited under the leadership of the South. That is surprising information, and it must be conceded in the current climate that is potentially threatening.

**National security and Electronic Media**

The notions of «national security» and the electronic digital computer are approximately of the same age, both products of World War II. ENIAC, the world's first digital electronic computer, went into service at the University of Pennsylvania in 1946. The U.S. government's Central Intelligence Agency and National Security Agency were launched a year later, authorized by the National Security Act. Until recently, national security and computers enjoyed a structural relationship. In the mid-1960s, perhaps even later, the chief U.S. government agencies responsible for national security were also the chief catalysts and funders for computer research, and also the largest customers of the computer industry. It has been asserted by experts that the appearance of the digital computer even shaped the strategy of national security in the United States, as more and more national security planning became dependent on computer-based models using techniques of systems analysis and operations research. One might even argue that this structural relationship between computers and national security is the primary bearer and symbol of U.S. power in the latter half of the twentieth century, even more so than nuclear weapons.

Computer technology has become the most important to national security. As a fact, without computers, modern arsenals and «battle management» and communications would be impossible. The present and the future appears to belong to what is so-called «smart» weapons, complex systems of command and control, telecommunications, satellites, electronic surveillance, and split-second information processing. The end of the Cold War has appeared to speed up the process of integrating advanced computers into weapons and command systems, rather than slow it down. The United States' overwhelming superiority in information technologies has been the key to its superpower status thus far.

However, a new phenomenon is the threat to national security posed by networked computers, particularly through the internet and cyberlinks. This is accompanied by more than a small amount of irony, as the internet was, for decades, a project of the U.S. Department of Defense. For a long time, during the period when the Internet was used almost exclusively by scientists, engineers, academics, and a handful of military personnel, the internet was viewed by experts mainly as a benign and interesting research project, one with modest and limited application to national security objectives. But in the past two to three years, the Internet has increasingly been regarded by national security officials as a new playing field for international conflict, a new medium in which national security will take on new forms, and one in which the U.S. government agencies responsible for national security have a growing stake. High officials of the CIA, the National Security Agency, the FBI, the White House, and other, less well-known agencies, and especially after the scandal generated by the Wikileaks, now believe that the internet is a «critical national asset» that requires their attention and protection. This may signal a new era in the development of the internet and digital media, equal in importance to its commercial potential. In fact, the commercial use of the internet may be influenced by national security controversies as much as by consumer response to new Internet applications.

There is a persistent myth surrounding the history of the Internet that it was designed to «sustain a nuclear attack», and that this was the chief research interest of the Internet's Pentagon sponsors. As described in the definitive history of the Internet, when wizards stay up late, by Katie Hafner and Matt Lyon, the story that lies behind this myth is somewhat complicated[[2]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn2" \o ").

Paul Baran, a RAND Corporation researcher who joined that Air Force-sponsored think-tank in Santa Monica, California, in 1959, «developed an interest in the survivability of communications systems under nuclear attack», writes Hafner and Lyon. «He was motivated primarily by the hovering tensions of the cold war, not the engineering challenges involved. However, Baran knew, as did all who understood nuclear weapons and communications technology, that the early command and control systems for missile launch were dangerously fragile»[[3]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn3" \o ").

While Baran's work was motivated by the goal of building a communications network that could survive a nuclear war, this motivation was only a small part of the flow of ideas that built the technical foundations of the internet. Even more important is the fact that the internet was never linked to any critical military application or system. The internet never played a role in controlling nuclear weapons, for example. The communications network that connected U.S. nuclear facilities, such as between the North American Air Defense Command in Cheyenne Mountain, Colorado -the hub of the country's «early warning» system- and the launch control headquarters of the Strategic Air Command in Omaha, Nebraska, was deliberately isolated from the internet.

For a variety of reasons, the development of the internet, even when it was funded by the Pentagon, scarcely attracted the attention of military planners or national security officials. And, ironically enough, it was this very openness of the internet's development that reduced its importance in the eyes of career military officers and high national security officials, who were conditioned to believe that anything significant in their fields must be classified and secret.

In short, while the Internet and the concept of «national security» share common roots in history, they developed along separate and divergent paths. This makes it all the more interesting that these paths are now converging again, but in a way that makes the internet problematic and even threatening to national security. A good example on that is the Wikileaks.

**Intersection of National Security and the Internet**

In February, 1998, U.S. Attorney General Janet Reno unveiled a $64 million plan to build a new «command center» to fight «cyber attacks» against U.S. computer systems. This new «command center» is called the National Infrastructure Protection Center, a Justice Department response to the report from the President's Commission on Critical Infrastructure Protection[[4]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn4" \o ").

These are just some of the more recent and visible results of concern over «cyber war», «infowar», «cyberterrorism», and other, related threats now perceived by law enforcement personnel and national security officials as new and important terrain. And these authorities commonly view the internet as the «highway» upon which these threats will be borne, again the case of Wikileaks.

The character of the internet has been dramatically transformed over the past few years, as everyone knows. What began as a communications network is now a vast, global, communications medium that rivals the public telephone network, television broadcasting, and even radio. The internet-using population, worldwide, is now over 650 million people, and Matrix Internet Data Services, an internet demographic consulting company in Austin, Texas, has predicted that, by the year 2012, there could be more than a Billion people using the network. Senior executives in large telecommunications companies, an industry which is now the largest in the world, routinely report that data traffic will soon surpass voice traffic, and that, packet-switched networks, like the internet, may eventually supersede the circuit-switched telephone network worldwide. The internet «model», of packet-switching, distributed communication, and unmanned digital nodes, appears to be the bedrock for nearly all future communications.

Of particular importance to those charged with national security is the fact that increasing levels of international commerce are conducted over the internet, and also increasing levels of government service. International funds transfers, now surpassing over a trillion dollars a day, are carried by computer networks. Power grids, banks, government databases, large corporate enterprises, news networks, transportation facilities, and many other essential components of civilized life are increasingly «on the net», delivering services or conducting critical communications over the Internet.

Disruption of such services or communications could, someday it is feared, resemble or approach in severity an actual physical attack such as a military strike or a major terrorist incident. What is important now, however, is that officials of the U.S. government and experts in the private sector are arguing, persistently, that the growth of the internet, and its expanding capabilities, combined with the fact that it is increasingly embedded in «critical national infrastructures», makes protection of computers on the internet a matter of national security. In other words, regardless of the current threat, the future indicates growing vulnerability and thus a growing urgency for protection and attention.

Jamie Gorelick, U.S. Deputy Attorney General, told the host of TV's «Nightline» news talk show, Forrest Sawyer, in December of 1997, «My own assessment, Forrest, is that we have a couple of years before there is a really serious threat. We have seen indications in criminal activity, in the plans of foreign nations, in the plans of terrorist groups that lead us to believe that we should be about the process of hardening our computers against attack»[[5]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn5" \o ").

In yet another irony, what may contribute to the threat of computer attack in the U.S. is the country's unrivaled military superiority. General Marsh said on the same «Nightline» program, «Nobody around the world today would attempt to defeat us on the battlefield. Instead, they will be seeking means to find vulnerabilities in our systems that they can exploit and do serious harm without having to confront us in the conventional armed way of the past»

If the Internet does prove to be a viable means for nations, groups or individuals to attack one another, nations capable of such threats will be able to afford a credible threatening status far more cheaply than if they needed vast arsenals of missiles and tanks. A relatively modest investment in the skills of a handful of network trespassers and hackers would become a substitute for immense investments in weaponry. As such, the sources of credible threats could proliferate.

It is important here to highlight that this «new terrain» of computer warfare or cyberterrorism poses some serious and unfamiliar challenges to national security authorities and for the following reasons:

First, all forms of warfare in the past have involved a threat to geographically specific assets by equally geographically specific threats - such as massed armies or ballistic missiles. One of the chief characteristics about computer attacks is their ambiguity in nearly every dimension: it's difficult to ascertain where the attack is coming from, who is behind it, what the motive is, whether it is the work of a determined enemy or merely a curious trespasser, etc. Penetrations that come from trespassers inside the U.S. may not be benign or «domestic» Before the war in the Persian Gulf, for example, there was a report of a U.S. hacker breaking into Pentagon computers and then offering to sell the information to Saddam Hussein (who didn't buy it because he didn't believe it was genuine)[[6]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn6" \o ").

It's not even clear what the term «cyberwar» describes. If it means an organized and coordinated attack on computer systems by another state government, that may be too high a threshold; it's unlikely we'll see an unequivocal example of this soon, except perhaps by the U.S. attacking an enemy's computers. «Cyberterrorism» may be more likely, but, as in the distinction between war and terrorism by other means, this prospect might call for solutions different than protection from «cyberwar»

Second, the United States has historically avoided major military attacks because of its relative isolation from belligerents, a kind of «continental defense» Most of the country's history in military strategy has been to keep conflict as far from the U.S. mainland as possible. But the internet poses a new dilemma: its global character, and the way it works, allows easy access to almost any networked computer inside the United States, including those running critical systems, from nearly anywhere else in the world. For a determined adversary, there are now millions of entry points to the U.S. heartland, and requiring no logistical effort, in contrast to the obstacles facing adversaries in the past.

Third, because of the fact that computer attacks can come from both inside and outside the U.S., and the fact that the origins of such attacks are difficult to identify promptly, jurisdictional controversies and overlap among law enforcement and national security agencies are already rampant. The U.S. has had a long tradition, for fifty years at least, of separating the jurisdictions of agencies responsible for domestic threats from those responsible for foreign threats. If the internet is factored into their responsibilities, these jurisdictional boundaries are rendered exceedingly vague and arbitrary, leading to confusion and conflicting interests.

Fourth, the biggest issue of all: for the most part, in the past, the U.S. military and its national security allies, such as intelligence agencies, have been charged with protecting military assets first, and using these as offensive weapons or deterrents against enemies. In a «cyberwar» scenario, however, conventional military assets will be useless, and there may be no appropriate offensive weapons available. The military and law enforcement and national security agencies are increasingly faced with protecting private assets, such as corporate computer systems, or other information systems far outside the jurisdiction of the federal government.

**The Internet threat to National Security**

While the question is obvious, the answer, unfortunately, is not. While advancing technology has made assessing all threats to national security increasingly difficult, assessments of the threat of «cyberwar» or «cyberterrorism» via the internet may be the most difficult of all, for a variety of reasons.

One of which is that the Internet is constantly changing. Indeed, it may be the most rapidly evolving entity in human history. It is difficult, if not impossible, to fix a «moment» on the internet to make an assessment that would last more than a few weeks, at most. This is very different than assessing other kinds of vulnerabilities or threats, which change or accumulate much more slowly. During the Cold War, U.S. intelligence sources had a reasonably good idea of the capabilities of the Soviet Union, at least in terms of the raw numbers of its military assets. It's difficult to imagine how the same sources could «count» the threat of Russian hackers, for example, some of whom have penetrated deep into the computers of U.S.-based banks, such as CitiCorp in New York?[[7]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn7" \o ")

Another, even if one were able to narrow one's focus to «critical» systems connected to the internet, there are no public or even readily available data on how vulnerable such systems might be. Defense computers are buried under layers of secrecy and classification, and private companies are not likely to volunteer such information. We typically only hear about computer vulnerabilities after a break-in, and even then we learn little about the incident, and sometimes the descriptions of break-ins are not accurate, either. As an example and this is at the time spread news, a New Jersey State Trooper once told the press that a teenage hacker he had arrested was altering the orbital paths of U.S. defense satellites, which was not only untrue but absurd.

But the overall problem facing national security authorities is that this threat of Internet-based terrorism or attack, however grave it might be, is to date not at all tangible to the average citizen. It is likely to become more so in the near future especially after the Wikileaks capturing of alertness among observers.

As everyone knows, «national security» is largely a game of perceptions, a combination of both real and imagined threats and assets. Even during the Cold War, it was controversial how big a threat the Soviet Union was to the U.S.; this controversy continues even today, nearly twenty years after the end of that conflict.

This controversy has put into belief the dual nature of the national security mission: the responsibility of such agencies to protect national technological assets and also retain the ability to intercept and interpret digital communications. In the era of the internet, these two responsibilities are in conflict with each other, thus posing significant dilemmas to national security officials. On the one hand, these agencies are urging businesses, other government agencies, and individuals to protect their computer data from attack. On the other hand, these agencies seek to control the way these people protect such data in order to protect law enforcement and national security agency access to this data. Not surprisingly, both businesses and individuals are hesitant to implement encryption schemes that require turning over keys to people they don't know or whose motives they don't fully comprehend. Because of this hesitancy, the first mission of the security agencies, that of increasing protection for U.S. computer systems, is obstructed[[8]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn8" \o ").

Another new phenomenon is the emergence of a new breed of «cyberlibertarians typically young, talented technologists who reject most of the assumptions of the national security establishment. Some of the more radical of these ideologues have argued that the Internet is the beginning of the end of the nation-state, let alone the end of the national security state. This perspective is not just an isolated intellectual discourse, either: the «cyberpunk» movement, for example, has complex and extensive ties to outlaw hackers, most of them young men, some of whom have adopted the intellectual framework of «cyberlibertarianism» as an ideological justification for criminal penetrations of government computers, casting themselves as liberators in the digital revolution. Such «counterculture» attitudes are widely shared by educated young people all over the world, perhaps a natural attitude of young people rebelling against authority. But when this attitude is combined with the fact that these same people are the most technically adept in the world, and a number of them are affluent or even wealthy because of this skill - once again, national security officials are confronting a new and alien environment, one dramatically different from eras of the past, when business leaders and skilled technologists were typically undisturbed by the alleged imperatives of national security. When confronting young leaders of the digital revolution, nowadays, national security people feel that they are facing hostile territory. The end of the Cold War has given new impetus to calls for a dismantling of national security institutions, and the Internet, with its idealistic potential for global communications between planetary citizens, has come along at just the right time to fuel such ideas. Widespread uses of phrases like «the digital revolution» and «Third Wave civilization» reinforce the popular notion that the «information age» entails an overturning of old regimes, including, perhaps, the centuries-old competition between nation states[[9]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn9" \o ").

It may seem grandiose to suggest that complex technical debates such as those surrounding digital encryption or the prospect of «cyberwar» are the most important political debates of our time. But this is in fact the case. This is not actually all that surprising, when one considers the catalyst of such debates: the Internet itself, one of the most remarkable, promising, and at the same time troublesome creations of human enterprise in the history of the world.

National security authorities, like everyone else, are confronted with a world far different than the familiar one of just a few years ago. The tripartite combination of the end of the Cold War, the new intensity in global commerce and competition, and the information revolution has served to upend almost all previous cognitive models about how the world works. National security bureaucracies, of course, are notoriously resistant to change. But they also have many arguments on their side, as new threats have appeared simultaneously with new ways of communicating and doing business.

National security experts are facing several frustrating dilemmas. First is the need to secure U.S. computer systems while retaining some ability to intercept and interpret digital communications. As many people have pointed out, this dual mission may not only be irreconcilable, but the effort may produce some absurdities and unacceptable impositions on people using computers or developing information technologies, particularly software.

Thus the implications of several initiatives by the national security community are so time-consuming, and so out of touch with the imperatives of the digital economy, that their chances of becoming law in the United States appear to be slim. Lawmakers dislike alienating national security authorities, but in this case they may have no choice. The economic health of the United States could be seriously damaged by several of the proposals now on the table.

Moreover, it appears that uncontrolled public key encryption algorithms are proliferating, despite the resistance of the U.S. government. «Key escrow» systems such as those advocated by U.S. government officials are too vulnerable to compromise, and once keys are released into circulation, all encrypted data is compromised. Public key encryption schemes are already available in a wide variety of products and on the Internet, and there doesn't appear to be much that the government can do about these programs[[10]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn10" \o ").

Today, the internet as a component of electronic media is regarded as one of the most important determinant of the human condition[[11]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn11" \o "). Nicos Poulantzas noted that «what is specific to the capitalist state is that it absorbs social time and space, sets up the matrices of time and space, and monopolizes the organization of time and space that become, by action of the state, networks of domination and power. This is how the modern nation is the product of the state»[[12]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn12" \o "). Manuel Castells maintains that electronic media has changed this paradigm as it challenges the state's ability to capture historical time through the appropriation of tradition and the construction and reconstruction of national security. Securities are originated from dominant institutions and become instrumental only when and if social actors internalize them and construct their meaning around this internalization.

In these global times, people are being exposed to diverse possibilities. The expansion, speed, and availability of international trade and global electronic mass media are exposing foreign cultural products and services, different perspectives and experiences at the local level; migration and people moving their cultures across borders, are all causing changes in local cultures, values, and traditions; producing multiple, fragmented, and cosmopolitan identities which can undermine national security.

Castells argued that «our societies are increasingly structured around a bipolar opposition between the Net and the Self[[13]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn13" \o "); however this system has not been able to give meaning to people's lives that's why they increasingly seek meaning through particularistic identities based on ethnicity, religion, regionalism or nationalism and this explains why many contemporary conflicts are not concerned primarily with 'rational' economic and social interests.

Because electronic media allowed for a higher mobility of people, Friedman noted, it has forced countries around the world to adapt to this new concept of multiculturalism and having to deal with problems of race and ethnicity. Consequently, one may ask if the social and political construction of national identities as the protector of national security, can take place without linking it to the concepts of territory and boundaries, and how can we understand the new relationship between the state and its political community, i.e. its citizens, in these transformative times.

Peter Mandaville noted that «the citizen is intrinsically linked to the state insofar as it is only the state which can bestow this status upon an individual[[14]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn14" \o "); this implies the notion of inclusion and exclusion in the sense that there are those considered to be citizens with rights and obligations as opposed to those who are non-citizens. The state has also traditionally served an important function that of the ethical in that it provides protection and social justice for its citizens. Both these structures have been challenged by the process of globalization manifested through electronic media.

As for the ethical function of the state, electronic media threatens the very essence of the Westphalian system: state sovereignty. The websites and electronic media of the transnational non-governmental organizations such as Amnesty International, Greenpeace, and Médecins Sans Frontières challenge state activities and its legitimate role to uphold the 'rule of law' within its territory as part and parcel of its sovereignty; they criticize and often attempt to interfere in situations of torture, detainment without trial, nuclear testing, and refusal to grant access to those offering humanitarian aid.

On the other hand, existing territorial states have become an amalgamation for economic interests and social identities within an intensely competitive, integrated yet unstable world economy. International corporations have gone beyond state boundaries to recruit labor and move them across borders, and the notion of the 'supra-state' such as the European Union, are both forcing a new form of political community based on a wider framework that of a global civil society.

However, as Mandaville argued, if we are to think that such «apparent inclusivity is highly democratic…there is also the sense in which such 'universalism' can be read as a form of exclusion which, by its assumption of homogeneity, negates difference»[[15]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn15" \o "). The integrity of the state is then challenged by those excluded groups classified under gender, sexuality, religion, ethnicity, and who are seeking their inclusivity under the notion of citizenship.

Stephen Castles and Alastair Davidson observed that globalization through electronic media broke the territorial principle, the nexus between power and place. Referring to the work of Lapeyronnie et al., they draw attention to the need of making a distinction between three elements that evolved in twentieth century 'national industrial society', these are: society, state, and nation. 'Society' referred to an economic and social system based on rational (as opposed to traditional or religious) principles within a bounded national territory; 'state' referred to a political system based on secular (and usually democratic) principles capable of regulating economic and political relations and change; and 'nation' referred to a 'people' defined on the basis both of belonging to the territory of the state and having a common cultural and ethnic background. Politics, the economy, social relations and culture were all congruent as they all took the nation-state as their main point of reference[[16]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn16" \o ").

Another vital distinction is the one between citizenship and nationality or as Castles and Davidson indicated, between «the notion of the 'citizen' as an individual abstracted from cultural characteristics and that of the 'national' as a member of a community with common cultural values» They maintain that the nation-state is the combination of a political unit that controls a bounded territory (the state) with a national community (the nation or people) that has the power to impose its political will within those boundaries, and that «citizenship is meant to be universalistic and above cultural difference, yet it exists only in the context of a nation-state which is based on cultural specificity – on the belief in being different from other nations»

However, when we examine the world as it is today, there are 200 nation-states in the world yet over 6000 languages – language being one of the indicators of a cultural community – hence conflict is bound to arise when different ethnic groups are to be molded within the confines of one nation or as D.P. Moynihan puts it, even if a fraction of these ethnic groups «were to seek to become nations, the potential for conflict would be enormous» He states that there is «an inherent contradiction between two basic principles of the United Nations (UN): the principle of national sovereignty and national security and that of the self-determination of peoples» (in Castles and Davidson 12).

The distinction made here between the nation and the ethnic group can be very ambiguous in that there have been several views and definitions of the 'ethnic' depending whether we look at the Anglo-American or the Continental European literature; consequently, maybe there need to be a separation between the concept of a nation and that of the state, thus a disconnection between nationality and citizenship. Still, in a world of migrants and ethnic groups, this entails reconciliation between the individual and the collective and a new notion of state borders (Castles and Davidson 24).

Anssi Paasi noted that boundaries do not limit themselves to landscapes and line demarcations; they manifest themselves in social and cultural practices and are instruments of social control and the communication and construction of meanings of identities. They link the past, present, and future together as they construct continuity for social interaction[[17]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn17" \o "). But when the existing landscape is reshaped and transformed by the actors within it and their interconnection with other actors outside of it; allowing for further spatial mobility of people, goods, money, ideas, technology, and other assets, the effectiveness of the state's authority and legitimacy in controlling and preserving its boundaries is brought into focus.

Some scholars believe that the stretching of social and economic relations across space and time has destabilized and weakened the nation-state. Huntington maintains that while states remain the primary actors in world affairs, they are also suffering losses in sovereignty, functions, and power. International institutions and powerful international bureaucracies now operate directly on individual citizens. In short, state borders have become increasingly permeable, and state's power and authority has been considerably weakened. Conversely, A. Amin and N. Thrift argue that «globalization does not represent the end of territorial distinctions and distinctiveness; rather it means an added set of influences on local economic identities and developing capacities» (in Newman 71).

Instead of being the end of geography, globalization then requires for us to reinterpret it away from the economic mapping of the world in terms of state territories, towards a more complex notion of states and localities integrated into the global economy. Political and social boundaries have not really disappeared; rather they have been reconstituted around and across long-established ones. People continue to experience a steady interconnectedness across geographical, cultural, and other divides even as they seek to maintain their distinctiveness and separateness from other individual communities.

In his attempt to locate political space under these changing conditions, R.B.J. Walker identified three transformations in the existence of our political identity/community: the first is related to the existence of a complex multitude of global connections; the second contends that the existence of these global connections does not necessarily entail some form of universalism; and third, that despite the global nature of these connections, people's lives are embedded in a myriad of particular locations and circumstances. He argues that «these three themes converge on recognition that in the modern world, communities and solidarities have to be grasped as a dialectical moment, as a sense of participation both in large scale global processes and in particular circumstances[[18]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn18" \o ").

Consequently, while nation-states seem to be loosing their power, they have not really lost their influence. People still live in closed worlds, the territorial state continues to be the dominant form of political organization in the minds of people everywhere; even in the case of dissatisfied 'ethnic' groups, and their goal generally is to get control of national governments or to separate and create their own. States and their boundaries remain a powerful source of identity in the modern world, especially at the level of the individual, and his/her participation in daily routine actions, which will continue to link them with the idea of sovereignty[[19]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftn19" \o ").

**Conclusion**

The global extension of the internet that is a natural and predictable development of computer networking was destined to clash with traditional principles of national security. Admitting this with the benefit of observation, of course, does not relieve the pressures of this clash that exist today, many of which are so vexing as to seem nearly insoluble. Two immense forces of great momentum are at odds: technological progress, which takes a million different forms, emerging from countless points around the world; and national security, the gravest and most fundamental public responsibility of the world's richest and most powerful nation. How the frictions between these forces will be resolved is not yet clear. Neither is likely to go away or even fade in strength.

There is a need to find a new definition for the concept of national security that can accommodate the internet. This does not have to be a radically libertarian utopia, one in which the nation-state itself withers and dies, as seems to be the hope of some young cyber-activists. Nor does it need to be an accommodation in which national security and police surveillance and enforcement are the rulers of the internet. Any new accommodation would probably need to take uncontrolled, public key, so-called «strong» encryption for granted, as this seems to be inevitable. National security authorities were once faced with another technological revolution of comparable significance and that is, intercontinental ballistic missiles with nuclear warheads, and security policy managed to adjust, for better or worse, to this new technology. The same kind of adjustment will now be required. The «national security state» that was a product of the Cold War may no longer be recognizable in ten or twenty years, but neither will any other institutions of modern society, because of the changes tied to the internet. Because of this, national security officials need to start thinking in fresh ways. Right now they're on the wrong side of history, as noble as their aims might be.

References

- [Gary Chapman](http://www.utexas.edu/lbj/21cp/bio.html)is director of The 21st Century Project at the LBJ School of Public Affairs at the University of Texas at Austin.

- Aviation Week and Space Technology, special issue on «Information Warfare», January 19, 1998.

- Cummins, Guylyn R., «**National Security Alone Can't Be Used To Censor Cryptographic Speech On The Internet**», Daily Transcript, March 12, 1997, available at [http://www.sddt.com/reports/ 97reports/iWorld97\_03\_12/DN97\_03\_12\_ti.html](http://www.sddt.com/reports/97reports/iWorld97_03_12/DN97_03_12_ti.html).

- Diffie, Whitfield and Susan Landau, «**Privacy on the Line: The Politics of Wiretapping and Encryption**», the MIT Press, 1998.

- EPIC, Electronic Privacy Information Center, «**The Computer Security Act of 1987**», at <http://www.epic.org/crypto/csa/>.

- Glave, James, «Critics Bash Reno's Cyberwar Plan», HotWired News, February 27, 1998, available at [http://www.wired.com/news/news/technology/ story/10605.htm](http://www.wired.com/news/news/technology/story/10605.htm)l.

- Hafner, Katie and Matthew Lyon, «Where Wizards Stay Up Late: The Origins of the Internet», Simon and Schuster, 1996.

- Nightline (ABC News TV talk show), December 9, 1997. Transcript available at [http://www.infowar.com/CLASS\_3/ class3\_011298a.html-ssi](http://www.infowar.com/CLASS_3/class3_011298a.html-ssi).

- Pale, Predrag, «Personal interview with the Croatian Deputy Minister of Science and Technology», Predrag Pale, March 16, 1998, Zagreb, Croatia.

- Stoll, Clifford, «**The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage**», Doubleday, 1989.

- Wayner, Peter, «**Computer Privacy: Your Shield? Or a Threat to National Security?**» The New York Times, September 24, 1997.

- Castles, Stephen and Alastair Davidson, «**Citizenship and Migration, Globalization and the Politics of Belongings**», MacMillan Press Ltd, 2000.

- Castells, Manuel. «The Information Age: Economy, Society, and Culture. Vol. II. The Power Of Identity», Blackwell Publishing, 1997.

- Friedman, Thomas L. «The Lexus and the Olive Tree», Anchor Books, 2000.

- Gills, Barry K. ed. «Globalization and the Politics of Resistance», Palgrave Publishers, 2000.

- Gort, Jerald D, Jansen, Henry, and Hendrick M. Vroom. Ed. «Religion, Conflict and Reconciliation», Vol. 17, Amsterdam, Rodopi B.V. editions, 2002.

- Hay, Colin and David Marsh, «**Demystifying Globalization**», Palgrave Publishers, 2001.

- Huntington, Samuel P., «The Clash of Civilizations and the Remaking of World Order», London, Free Press, 2002.

- Klare, Michael T., «Resource Wars. The New Landscape of Global Conflict», New York, Holt & Co., 2001.

- Mandaville, Peter, «Transnational Muslim Politics», Routeldge, 2001.

- Newman, David, «Boundaries, Territory and Postmodernity», Frank Cass Publishers, 1999.

- Robertson, Robbie, «The Three Waves of Globalization, A History of Developing Global Consciousness», Zed Books publishers, 2003.

- Robertson, Roland, «**Globalization: Time-Space and Homogeneity-Heterogeneity**», in M. Featherstone, S. Lash and R. Robertson (eds.) Global Modernities, London: Sage, 1995.

- Rochester, J. Martin, «**Between Two Epochs, What's Ahead for America, the World, and Global Politics in the Twenty-First Century»**, New Jersey: Prentice Hall, 2002.

- Viotti, Paul R. and Mark V. Kauppi, «**International Relations Theory: Realism, Pluralism, Globalism, and Beyond**»,  New York: MacMillan Publishing Company, 3rd edition, 1999.

[[1]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref1" \o ")-     Jane Young, Fall-out from the leak fairy. Published: 12:05PM Friday December 03, 2010 Source: Pundit.

[[2]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref2" \o ")-     [Hafner and Lyon, 1996](http://www.utexas.edu/lbj/21cp/isoc.htm#Hafner#Hafner). http://www.utexas.edu/lbj/21cp/isoc. htm/Hafner/Hafner.

[[3]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref3" \o ")-     http://www.utexas.edu/lbj/21cp/isoc. htm/Hafner/Hafner.

[[4]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref4" \o ")-     Ibid.

[[5]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref5" \o ")-     http://www. .utexas.edu/lbj/21cp/isoc. htm/Nightline/Nightline.

[[6]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref6" \o ")-     1997, http://www. .utexas.edu/lbj/21cp/isoc. htm/Nightline/Nightline.

[[7]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref7" \o ")-     http://www.utexas.edu/lbj/21cp/isoc. htm/Glave/glave, 2009.

[[8]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref8" \o ")-     http://www.utexas.edu/lbj/21cp/isoc. htm/Glave/Glave.

[[9]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref9" \o ")-     http://www.utexas.edu/lbj/21cp/isoc. htm/Stoll/Stoll.

[[10]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref10" \o ")-    http://www.utexas.edu/lbj/21cp/isoc. htm/Pale/Pale.

[[11]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref11" \o ")-    http://www.utexas.edu/lbj/21cp/isoc. htm/EPIC/EPIC.

[[12]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref12" \o ")-    Castells, Manuel, «The Information Age: Economy, Society, and Culture»,

        Vol. II, The Power of Identity, Blackwell Publishing, 1997. p. 243.

[[13]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref13" \o ")-    Castles, Stephen and Alastair Davidson, «**Citizenship and Migration, Globalization**» and the Politics of Belongings. MacMillan Press Ltd, 2000. p. 6.

[[14]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref14" \o ")-    Mandaville, Peter. «Transnational Muslim Politics». Routeldge, 2001. p. 12.

[[15]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref15" \o ")-    Ibid, p. 13.

[[16]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref16" \o ")-    Ibid, p.p. 6-7.

[[17]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref17" \o ")-    Newman, David. «Boundaries, Territory and Postmodernity», Frank Cass Publishers, 1999. p. 72

[[18]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref18" \o ")-    Mandaville, Peter. «Transnational Muslim Politics. Routeldge», 2001, p. 27.

[[19]](https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy" \l "_ftnref19" \o ")-    Newman, David, «Boundaries, Territory and Postmodernity», Frank Cass Publishers, 1999. p. 71.

**الأمن القومي، وسائل الإعلام الالكترونية والسياسة الخارجية**

في السعي إلى تحديد سياسة الدولة والمصلحة الوطنية والسياسة الخارجية يعتبر الأمن القومي نقطة الانطلاق لتحقيق هذا الهدف، إلاّ انه نظراً إلى اختلاف المصالح الجزئية وتعددها ضمن المجتمع الواحد، والتي يتضارب الكثير منها بعضها مع البعض الآخر فإن مهمات التوفيق بين المتعارضين هي من مسؤولية من يمثلون هذه القوى ضمن الدولة ومن يحتلون مناصب حكومية.  
يسمح هذا الأمر بتحديد الهوية بين أهداف الدولة والحكومة ويعتبر الأمن والرخاء من المظاهر الثابتة لأهداف الدولة. وغالباً ما تمارس الحكومات سياسات تمثل آفاق مشروع وطني خلال مدة حكمها فيما تعزز الدولة القيم الأساسية للسلوكيات.  
بالتالي فإن الأمن القومي والأهداف يحددان سياسة الدولة ويسمحان لنا بفصل الأهداف الثابتة عن الأهداف السياسية والعمل السياسي في نطاقهما الأوسع. من الواضح أن تحديد معنى «المصلحة الوطنية» لا يمكن أن ينحصر فحسب بوجهة نظر واحدة كما أن رؤية المحللين العسكريين أو القانونيين أو الاجتماعيين أو الاقتصاديين ليست شاملة بما فيه الكفاية لتدمج كل عناصر الفهم الشامل للواقع الحالي والسيناريوهات المستقبلية.  
خلال التطبيق أو خلال تطور المجتمع يحصل تبادل للمعلومات وتطورات بين الممثلين الداخليين والخارجيين المشاركين في الدينامية الاجتماعية.  
هذه المعطيات نوعية وقابلة للقياس وسمحت لنا في ظل عملية منهجية بالحصول على نظرة شاملة للواقع المحلي والدولي وعلى تحديد صحيح لمعايير الأهداف التي تصبح ثابتة أو للأهداف الاستراتيجية.  
وجهة النظر هذه يكون فيها ميزان القوى الوطنية المقاربة الأفضل عند تحليل السياسة الخارجية وقدرة الدولة على العمل لتحقيق أهدافها وما تسميه مصالحها وأمنها، ويسعى الأمن إلى تلبية الأهداف الأساسية الضرورية لبقاء الدولة.  
هذا الأمر مهم للتشديد على الأهداف والمصالح الوطنية والحصول على معنى نظري.  
ثمة معتقد تقليدي يقسم القوى في 4 حقول ويمكن إدراجها كالآتي:  
- السياسة التقليدية  
- الاقتصادية  
- النفسية – الاجتماعية  
- العسكرية  
لا يجدر بهذا التقسيم ان يقودنا إلى اعتبار أن معالجة الموضوع تتم وكأنه شيء جامد متناسين أنه ثمة علاقة دينامية قائمة بين هذه المكوّنات في المجتمعات البشرية.  
«حقول القوة» هي أطر تشمل النشاطات المترابطة بعضها مع البعض من حيث طبيعتها وهي مفيدة للتحليل.  
وتقتضي الطريقة الاعتيادية تشخيص الواقع السياسي بمعناه الواسع لتضمين مجموعة العلاقات الاجتماعية ضمن الدولة والأهداف الإستراتيجية والسياسية وفق المصلحة الوطنية والمخزونات الاستراتيجية والتشخيص الاستراتيجي، كما أن تشفير المعلومات وتحويلها إلى معارف هو أمر مفيد وأساسي لبقاء الدولة ولأمنها.  
بالانسجام مع هذا التقييم للأمن القومي فإن التفاجؤ مما تضمنته وثائق موقع ويكيليكس يعني أننا إما نتجاهل ما يحصل على النطاق الدولي، وإما أننا نثق بشكل ساذج بالحكومات، وإما الاحتمالين معاً.  
بالنسبة إلى الأمن القومي لا يعتبر أي من هذين الاحتمالين فضيلة.  
لم يعتمد فن الدبلوماسية قط على التعامل الحسن والوضوح والصراحة بل هو بالأحرى عالم من المصالح والاتفاقيات والمجاملات المخادعة والمصافحات المتردّدة واللقاءات السرية والسياسات الضبابية والرشى والأكاذيب الفاضحة وكل ذلك لزيادة المصالح الوطنية والخاصة.

- See more at: https://www.lebarmy.gov.lb/en/content/national-security-electronic-media-and-foreign-policy#sthash.kb9WOrlB.dpuf