## French Institute for Strategic Analysis

## (Institut français d'Analyse stratégique, IFAS)

—

# Research Program 2013

# Section 1

## IFAS General Orientations

IFAS was created in 2001 by François Géré in order to bring together within the same team experts from the extremely various domains involved today in strategy and, more generally, in defense affairs: international relations, human, political and law sciences, dual use technologies. Our approach consists in merging fuzzy domains and "hard" sciences, and in crossing macro-strategic (global dimension of confrontations) and micro-strategic (local specificities of confrontations) approaches.

The main domains of research include:

- Analysis of present confrontations, especially guerrillas and terrorisms;
- Role of nuclear power in the world, civilian and military, along different directions: energy, strategy, proliferation, terrorist risk, etc.
- The "strategic triangle" China-USA-EU;
- Strategic role of ITC technologies, in time of peace, crisis, war, and also computer science, Internet science, Information Systems safety, political economy.

# Section 2

## The domain of Cyberstrategic Studies

This last domain, due to its recent fast evolution, is henceforth at a very special place among IFAS's works and researches.

Salient points and main research orientations are to be found below.

As every society oriented towards scientific research, IFAS has fellow members in various countries: USA, China, Russia, Israel...

IFAS is involved in various EU and NATO research programs.

The last section of this document introduces our team ; a more comprehensive presentation is to be found on IFAS's website: http://www.strato-analyse.org/fr/spip.php?rubrique2.

## 2.1 Structure and geography of Cyberspace

The spatial and topological structure of the Internet, as well as its division in distinct territories shared among powers, are basic facts useful to understand the confrontations which occur within it. On this topic, we are working with Prof. Kavé Salamatian, from the University of Savoie, and with Michel Volle. Prof. Salamatian has a great research curriculum on this topic. Michel Volle's works are mainly on the economic side of the issue.

Among others, the following papers may be read on line:

http://www.strato-analyse.org/fr/spip.php?article221
http://www.strato-analyse.org/fr/spip.php?article222
http://kave.salamatian.org/wordpress/?p=6

The Internet is made of some 5 000 networks, among which communications are on a peer-to-peer basis, it is they are not just another network's customers. Inside such a network, it's owner (in general an Internet Services Provider, ISP) establishes the rules which his customers have to obey. The Internet may be seen as a continent, where these networks would be the countries, with boundaries between them. Crossing these boundaries is submitted to rules established according to *transit agreements* between ISP. These agreements may be *peering agreements*, if the networks are peers, i.e. of similar size and turnover, or customer to provider agreements, where the customer is little in front of the provider. These agreements are implemented in *routers*, i.e. specialized computers simultaneously connected to several networks and able to transfer data flows from a network to another, in accordance with rules written in the *Border Gateway Protocol's* syntax (BGP).

As mentioned above, not all networks are peers. The biggest form the *tier 1*, and have peering agreements among them. The other have to buy their connectivity in order to access the worldwide Internet.

In optical fibers, data transfer speed is close to light speed, so physical distances may be considered as null, and more relevant distances may be measured as the number of routers between two points, or as the number of network boundaries to cross over.

The study of these relationships among networks, their topology, and the resulting balance of power, is the object of *cybergeography*, a science initiated by Kavé Salamatian.

## 2.2 Law and Economics

IT technologies and the Internet are challenging our understanding of economics. As noted by Michel Volle[1], "*Informatization* refers to the historical emergence of an alloy of *human being* and *ubiquitous programmable automaton* aka *computer*. Through Informatization, economy evolves since 1975 in an *iconomy*: increasing returns to scale in microelectronics, software and Internet result in a transformation of products, mode of production and distribution, organizations, market structure, competition and even the preferences of the consumers."

The emergence of *iconomy* is an industrial revolution, the third one after the one of the end of the XVIII$^{th}$ century (steam, mechanics, chemistry) and the one of the end of the XIX$^{th}$ century (electricity and internal combustion engine). This revolution has the power to disrupt the whole balance of power among nations, and the countries which won't learn the lessons from it will be condemned to decline and loss of independence.

With this prospect in mind, the control of *Internet Exchange Points* (IXP) is as crucial as was the control of the Dardanelles and Suez canal at the time of the second industrial revolution. To analyze these facts we have to understand simultaneously the economics of connections market, the technology of network protocols, and the geography of Internet's topological

1 http://michelvolle.blogspot.fr/2012/12/de-leconomie-liconomie-opportunites-et.html

structure. Michel Volle and Kavé Salamatian hold a strong leadership in this field of investigation.

## 2.3 Safety, freedom et prosperity

### The Internet, the Individual, the State

Today Internet's usage is widespread in (almost) all categories of population, including those of developing countries. This matter of facts results in some upheavals and unheard of problems in the fields of literacy, law, police and defense. Evidence of that is given, for instance, by the controversies about intellectual property (IP) and copyright management in many countries. Almost in every country the IP and copyright laws are to be renewed. Disputes about SOPA *(Stop Online Piracy Act)* et PIPA *(Protect IP Act)* in the US are just a beginning, as are disputes about the Hadopi (High Authority for Dissemination of Works and Protection of Rights on the Internet) in France.

Privacy stands as another major topic. From now on positioning systems of cell phones allow permanent tracking of individuals and database networking allows cross referencing of personal data, including biological and medical, on a scale which none of the dictators from the past century had even dreamed. More generally, the very principles of democracy are challenged by these transformations, and should be updated in some way.

Awareness of the geographic location of one's data and their processing in the Internet is more and more difficult, especially with the generalization of Cloud computing. In the Cloud, virtual machines (VM) may migrate and even multiply at any time, anywhere, even abroad in countries with different laws regarding the protection of privacy, the confidentiality of the data, intellectual property, etc. Kavé Salamatian's idea to redefine Internet as an extra-territorial space supervised by a specialized UN agency (not ITU) may win recognition, but then the terms and modes of enforcement remain to be established.

These topics raise the matter of identity management in the cyberspace: electronic signature, certificates, key escrow. Technical solutions exist, but are not perfect, for instance recognized certification authorities like DigiNotar and GlobalSign have been compromised. The technical side of the question is not the only one: acceptance of anonymous transactions and authoring on the Net is controversial, as is the idea of mandatory authentication.

These matters need contributions by researchers in social sciences, law sciences and economics, beside computer scientists, cryptologists and strategy specialists.

## 2.4 Towards cyberwars?

That topic has become fashionable and has triggered volumes od articles, opinions. That will continue without providing better understanding of the problem.

However it is a major issue which need a carefull and well documented approach.

If cyberspace, defined as the set of data open to Internet access and their transfer flows, is obviously and simultaneously at stakes of confrontations and the place of acts of confrontation;

If almost everybody agrees that an attack committed exclusively in cyberspace could not have strategic deciding results as to destroy enemy capabilities, at least today, many questions remain open:

- If a democratic country needs obviously defensive capabilities in cyberspace, should it develop cyber attack capabilities? Is it possible to create valuable defensive capabilities without offensive skills?

- If there are many decisive reasons making attribution of cyber attacks to their author very difficult, to which extent is it possible to overcome them, or, to put it in another way, which success rate could we expect for an attribution?
- Tightly correlated to the previous question is the following one: which are the ways open to develop a cyber deterrence strategy?
- We need to transpose in cyber context the classical strategic dilemma: between defense and offensive, which one has the advantage over the other?
- Should retaliation against a cyber attack stay in cyberspace, or could it take conventional ways? And if the second alternative is accepted, how to establish thresholds to start each level of retaliation?

At the same time the spectrum of organized armed conflicts (political violence) is much broader and complex than the interstate wars as we experience more and more since the end of the Cold War. To the forefront have arrived the so called low intensity conflicts including civil wars which, as demonstrated by the recent case of Syria can produce a high number of fatalities. Insurgency and subversion using guerilla and terrorism are spreading. They use as a major weapon information and disinformation warfare through Cyberspace.

More and more often cyber terrorism is mentioned as a potential threat. To be sure, so far, it has never been used in a professional manner at a high scale of lethality. Many consider that it will strike precisely where and using procedures we are not thinking of. However at present terrorist organizations use the Internet to get “revolutionary taxes” from the targeted companies they are traditionally blackmailing. They don’t need any longer to kidnap people to get the ransoms.

In the case of domestic upheavals the use of the many social networks which are now at hands are systematically used on a large scale. Facebook or Twitter helps organizing demonstrations. They also can be used by police forces to mislead and bring total confusion among the opponents. Finally, cyberspace helps creating a global awareness of what is going on. It may trigger the action of the international community. It may not (Iran 2009, Syria since 2011).

Those different forms of struggles, *modus operandi* and the related tools are not yet considered by international organization. Problems are too new, the stakes too high and too complex. Therefore Cyberspace is generally considered a virtual jungle where law has not yet penetrated. That view is far from being correct. Nonetheless, despite some limited initiatives such as the 2001 Budapest convention (see below), domestic and international legislations are lagging precisely because no State can consider entering into international legally binding agreements before it has established its own legislation.

Those are the key issues cyberdiplomacy will be looking at.

## 2.5 *Cyberdiplomacy* : the might and the right

Here we introduce a new domain of activities and a field of research studies *Cyber diplomacy* as a major component of Cyberstrategy.

That field consists in the examination, understanding of the diplomatic posture of all the parties (i.e all the States but also the different groups and NGOs) interested in the regulation of Cyberspace according to their interests and their visions of the future.

The key goal of cyber diplomacy is to identify the major tools which could contribute to shape the cyber environment, to prevent conflicts, to deal with them, to avoid dangerous confrontations, including war in Cyber and war through Cyberspace. According to the kinds of items considered and the degree of good will of each actor, there are indeed many paths and many steps: confidence building measures, good practices and fair conduct agreements.

Beyond the analysis of the recent and forthcoming diplomatic activity: identification of the hurdles and stalemates. From our point of view cyberdiplomacy has to be inventive and put forward proposals about how to overcome them.

### *Cyberdiplomacy considers the role of international organisations*

It integrates the existing consultations and suggests paths to agreements among the different security organizations (EU, OSCE, OECD, Shanghaï Cooperation Organization, etc) according to their different nature and needs.

Cyberdiplomacy consists of the proposals and initiatives put forward by the different actors at the level of the United Nations (like the measures suggested by Russia) and the attempts to establish bilateral dialogue between the US and China. Cyberdiplomacy studies will evaluate the quality and purposes of those proposals and will try to understand why so far they have been unsuccesful

## 2.6 Law and regulatory measures at the international level

Efficient diplomacy should be based upon legally binding agreements of various kinds, nature and duration which States have decided to agree upon in good will because they meet their interests

What is at present the legal framework established by the internation law? The Budapest Convention of 2001, which has not been ratified by many states, considers and defines criminal activities but does not address the relation between states. In order to make Cyberspace a “normal”, domain similar to land, sea, air and space, States will have to agree upon several major principles. Relevant and universal norms will help dealing with the many different situations: tension, crisis, war. In that ultimate case such norms would allow to establish the legitimacy of offence and defence.

Humanity is indeed entering into the long process of creating a brand new international right applying to that extraordinary domain both material and virtual, the cyberspace. To be established it should be able to reach universal agreement upon definitions such as: what is a cyber weapon? What is a hostile process / malicious procedure? What is a major aggression versus a simple attack?

Then, can we use and apply the traditional principles which have structured for centuries war and peace such as the right of self defense? Can they apply to the immateriality of the Cyber since no territory is invaded by armed forces, no frontiers are violated. Even under such circumstances, the responsibility of the initiative of the aggression remains difficult to establish. It is often complicated because of the notions of prevention and preemption which make the debate very confusing. Henceforth the implementation of treaties and the interpretation of the working mechanisms of traditional Alliances are at stake. For instance, how **neutrality** can apply and be used since the territorial domain remains immaterial? In other words at present a defense treaty which would neglect the response to cyber aggression would be *de facto* obsolete.

How simply do or can we apply the traditional notions of *jus ad bellum* et de *jus in bello* ? How relevant are they in cyberspace ? According to which criteria the proportionality principle should be evaluated ?

So far several proposals have already been put forward in an uncoordinated manner bearing more risks of confrontation rather than real sound cooperation.

Cyberdiplomacy is to be developed in close connection with other research domains, particularly those mentioned in Section 2.3, which are dealing with human security and the conservation of privacy and individual freedom.

That concern deals with the delicate balance between the respect of the rights of the average Citizen versus the non ordinary State.

# Section 3

# The team

The *Institut français d'Analyse stratégique* (French Institute for Strategic Analysis, IFAS) is a multidisciplinary research team with experts in the fields of strategy, international relations, economics, management, computer and Internet science, information systems and law.

- François Géré, principal investigator in strategy and international relations, president of IFAS (http://www.strato-analyse.org/fr/); author of many books and articles about nuclear proliferation and deterrence, psychological war, and terrorism;
- Michel Volle, economist and statistician, one of the founders of the French school of data analysis, co-chair of Institut Xerfi (http://institutxerfi.org/), expert in Information Systems; author of many books, articles, a Web site (http://volle.com/) and a blog (http://michelvolle.blogspot.fr/);
- Kavé Salamatian, full professor of computer science and networks with University of Savoie (http://www.polytech.univ-savoie.fr/index.php?id=listic-kave-salamatian&L=0), fellow member of the Chinese Academy of Sciences, advisor of great Internet companies (Cisco, Huawei...); author of many scientific articles **(http://kave.salamatian.org/wordpress/?p=10) ;**
- Hervé Schauer created his own Networks Security Consultants firm (http://www.hsc.fr/index.html.en) in 1989; among his customers are the biggest French and European businesses; he is a worldwide renowned expert, with many articles and reference books (the list is here: http://www.hsc.fr/societe/herve_schauer.html.en);
- Laurent Bloch was the IT Director of INED (National Institute for Demographic Studies), CNAM (French Open University), Pasteur Institute, Paris-Dauphine University, and the Head of Computer Security at Inserm (French NIH); author of some reference books and a Web site (http://www.laurentbloch.org/MySpip3/) devoted to Computer Science and Information Systems Security;
- Olivier Danino is a Doctoral Student with François Géré; he published some excellent papers, especially about strategy and geopolitics of the Middle-East;
- Lars Wedin, graduated from the Defense College in Stockholm and from the High School of Naval Warfare in Paris, author of books and articles, especially about Naval Warfare;
- Thierry Widemann, historian specialized in compared military history of Antiquity and of the XVIII$^{th}$ century, expert in strategic theory;
- David Rigoulet-Roze, graduated in Political Science, International Relations and Geopolitics, author of books and articles, mainly about geopolitics of modern and contemporary Middle-East;
- Philippe Wodka-Gallien, graduated from the Institut d'Études Politiques in Paris, author of many articles, especially about military usage of bleeding edge technologies.