The new geopolitical coordinates of cyberspace - As novas coordenadas geopolíticas do ciberespaço

Professor
Armando Marques Guedes

> "Rather than focusing exclusively on the shifts of power among nations, or the shifts of power between some nations in particular, our focus should first be upon the shift in power that the rise of this architecture called cyberspace creates. How it now represents a source of power, and how the character of that power gets determined by its design.[…] Struggles of power get played out upon this stage set by the architecture of the space. Whether states have power, and how much; whether competitors have power over other competitors and how much. An account of international relations that ignored this stage would be as incomplete an account as one that ignored China".
>
> Larry Lessig (2000) "Architecting for Control",
> Keynote Address, Internet Political Economy Forum,
> *Cambridge Review of International Affairs*, Cambridge, UK. May 11

The present article[1] seeks to raise a few political questions on the current state of cyberwarfare in international relations and its impact in military doctrine - as well as point out some of their geopolitical implications. It focuses mostly on the political dimensions of cyberspace and on its agonistic topographies. Russia, China, North Korea, the US, Germany, the UK, Japan, Brazil, and non-State entities like al-Qaeda, are patterning that space. But so are anonymous hacker geeks wikiing their way upwards on open source software development, the famous "hacktivists": the germs of a 'virtual international civil society' often bent - and with the most varied motivations - on 'direct political action'. Given the nature of new digital communication technologies, their 'networkiness', and the empowerment they thus re-distribute, the discussion branches out to social networks, collaboration and surveillance, and some of the trends of

contemporary politics which resonate with them. No sustained attempt is made to produce a 'theory': the paper's main thrust is on 'revealing' - in the sense of bringing out a photographic image - emergent and germane political entities and their forms of operation. The aim is to begin drawing what are deemed to be some relevant geopolitical coordinates of a cyberspace which is rapidly rising on the scene of modern national and international conflicts.

Hybrid cyberwarfare and the paradigmatic case of Georgia

Recent years have shown us how central "cyberwarfare" has become. The complexity of the challenge has also been brought to light. One example will suffice to bring out some of the political aspects of such complexity. In the case of the so-called "Five-Day War"[2], the Russian invasion (quickly followed by a dismemberment) of Georgia, successive waves of attacks were launched - and waved around before, during and after the August 2008 invasion - on servers in Georgia.

In fairly general terms, here is how things went. As the official Report of the Georgian Government entitled *Russian Invasion of Georgia. Russian Cyberwar on Georgia*[3], explains it, "[t]he Russian invasion of Georgia was preceded by a cyber attack on Georgia's Internet facilities. A large number of Georgia's Internet servers were seized and placed under external control from late Thursday, 7 August, whereas Russia's invasion of Georgia officially commenced on Friday, 8 August. Also, much of Georgia's traffic and access was taken under unauthorized external control at the same time that this first large scale attack occurred". There were various targeted sites, all carefully chosen - as clearly the objective was to hinder the communicational and internal and external coordination capacities of the Georgian State and its allies. As the report put it, "36 important web sites were identified as targets for hackers, including the US and UK Embassies in Tbilisi, Georgian Parliament, Georgian Supreme Court, Ministry of Foreign Affairs, various news agencies and other media resources, the Central Election Commission, and many others".

Who designed and who launched these attacks? It appears different actors did different things. Interestingly, although initial target-choices were 'centrally-planned', strikes came from various different sources and flowed in a sort of curiously decentred pattern - and they followed a variety of tactical paths. Allow me to quote analyst Nick Farell at some length[4]: "[the hackers carried out a] kind of attack, known as a distributed denial of service attack, is aimed at making a Web site unreachable. It was first used on a large scale in 2001 to attack Microsoft [which neutralised, among countless others, such giants

as Yahoo, eBay and CNN] and has been refined in terms of power and sophistication since then. The attacks are usually performed by hundreds or thousands of commandeered personal computers, making a positive determination of who is behind a particular attack either difficult or impossible". As far as we know, in the case of Georgia, the stratagem used was not, however, merely that of a 'denial of service': "[i]nitially, security experts assumed that the sites were felled via "distributed denial of service" (DDoS) attacks, a well-known method of assault that uses hundreds or thousands of compromised personal computers to flood a targeted site with so much junk traffic that it can no longer accommodate legitimate visitors. But investigators soon learned that attackers were instructed in the ways of a far simpler but equally effective attack strategy capable of throttling a targeted Web site using a single computer. Security researcher and *Grey Goose* [a consortium formed at the bequest of the US Government for the purpose of looking into the cyber attacks on Georgian targets] investigator Billy Rios said attackers disabled the sites using a built-in feature of MySQL, a software suite widely used by Web sites to manage back-end databases. The 'benchmark' feature in MySQL allows site administrators to test the efficiency of database queries, but last year hackers posted online instructions for exploiting the benchmark feature to inject millions of junk queries into a targeted database, such that the Web servers behind the site become so tied up with bogus instructions that they effectively cease to function".

An innovation, then, and a serious one, as innovations go - albeit the problems in the case of the computer assaults against Georgian targets were not as severe as they could have been since, on one hand, many of the Georgian servers were immediately disconnected and their contents 'migrated' to servers overseas, and, on the other, given that many of Tbilisi's computer systems are 'primitive', and consequently not online, they were not neutralised.

There cannot be not much doubt the target-selection was a toil of Russian State institutions. But there is much debate as to whether the attacks were coordinated by the Kremlin or whether they were spontaneous and carried out by opportunistic Russian hackers. The relatively low virulence of the attacks, however, suggests the last of these hypotheses. What is more, many of the IPs the attacks originated from belonged to North American, French, Spanish, Latin American etc. addresses. Anyhow, it should be noted that sustained malicious swarm attacks occurred simultaneously with massive conventional military attacks - and the two types of strikes were carried out in a loosely synchronized manner.

What was the detailed assault pattern followed in the Georgian case - in terms of its 'political composition', or 'texture', so to speak? Was there only one well-coordinated military assault? Or was there a civil-military strike beforehand? Fascinatingly, what seems to have taken place was the progressive unfolding of a strongly *hybrid* action. And a very clear hybridity at that: although the participation of 'independent' hackers (congregated informally in what I will term a 'virtual civil society') seems indisputable in the case of the cyberwar against Georgia, everything appears to so suggest that the same

can be said of the active complicity of the Kremlin authorities. As political analyst Brian Krebs mentioned, Jeff Carr, the chief investigator of *Project Grey Goose* consortium, indicated that the site in which the addresses and recipes for attack were placed was suggestively named *StopGeorgia.ru*. The attack that was launched came up against Georgian defences but it succeeded in defeating them; and the idea that there has been a heavy degree of premeditation seems irrefutable. Let us listen to the very words of Brian Krebs[5]: "StopGeorgia administrators also equipped recruits with directions on evading those digital roadblocks, by routing their attacks through Internet addresses in other Eastern European nations. The level of advance preparation and reconnaissance strongly suggests that Russian hackers were primed for the assault by officials within the Russian government and or military, Carr said. The fact that the StopGeorgia.ru site was up and running within hours of the ground assault - with full target lists already vetted and with a large member population - was evidence that this effort did not just spring up out of nowhere', said Carr, speaking at a forum in Tysons Corner, Va., sponsored by Palantir Technologies, an In-Q-Tel funded company in Palo Alto, Calif., whose data analysis software helped Grey Goose investigators track the origins and foot soldiers involved in the cyber attack. 'If they were planning ahead of the invasion, how did they know the invasion was going to occur? The only way they could have known that is if they were told'.

So it appears that what we witnessed was a Russian State intervention, followed by a swarm of 'private' involvements, in a rather self-organized manner. What took place was the formation of a digital political movement of sorts, in this case *parasitical* [6] on State involvement.

What does all this mean - in what does it spell from a political angle, from the perspective of the development of new forms of politics? It denotes the emergence of new political-military coordinates, no doubt. This is one thing that we cannot afford to overlook. New coalitions appear to be emerging rather spontaneously - and it is something on which Russians and Chinese stand at the front line of innovation. If such is the case - and there is much to indicate that it indeed is - the political impacts of these kinds of more or less spontaneous coalitions should not be disregarded.

Indeed, such innovative forms of bellicosity raise questions related to the old responsibility-freedom binomial, once again on stage but now in *à la page* garbs. Notwithstanding the inevitable academic interest that will generate, we should however dig into the actual political and military significance and ultimate reach of the interventions carried out by these sort of 'metastasis' of a 'virtual civil society' of variable geometry, which continually forms and un-forms itself according to the specific causes. Although an answer to this clearly exceeds my scope here, that is obviously a matter worth pondering rather carefully. It is certainly worth our while to ask: are we witnessing the rise and rise of coalitions of the spontaneously willing? In any case, a new type of

‘direct action’ and ‘political participation’ seem to be emerging, with the format of unusual, or atypical, ‘political movements’ - clearly, not all ‘virtual communities’ are “herbivorous”... Could we be spectators of the beginning of personal, or “crowd-sourced”, foreign politics? And, crucially, if so, are we ready for this cutting edge form of policy ‘designing’?

The answer to this last question is yes and no. In general terms, States and international organizations can counter-act, at least temporarily and partially, network activists - by bringing to bear on them their superb organizational capabilities, acting in precise targeted manners and at well-calculated rates so as to slow them down. But does this mean States are sufficiently prepared to effectively face off future cyber-threats? Given institutional inertia and State propensity for ‘viscosity’ in strategic decision-making it is hard not to suspect theirs is, and will remain, little more than a piecemeal approach, thus condemned to fail in the long-run - unless the most threatened States display the necessary organizational learning they tend to be so inept at, and deeply reconfigure themselves into adaptive, networked, *relational* entities with little resemblance to the old 19th Century ones with which we still co-exist.

So a new game is afoot - something I shall want to come back to. The relatively recent January 2010 systematic and rather well synchronized attacks on Google and a host of major US corporations linked to defense and computer technologies, rapidly and easily traced back to Chinese IPs is a good case in point of a fresh trend we still do not fully understand - their origin kept sufficiently ‘unmasked’ for all to easily mark them out, arguably as a display, as one of the ‘loudspeaker foreign policy’ exercises of the swarm of assaults (on par with China’s very public shooting down of a satellite, a few months ago, in a open display of its novel anti-missile capabilities). Such attacks dove-tailed (and still do, in July 2010) the litigation between the Beijing and Google about the censorship Chinese Government insist on imposing on Google’s search capabilities for users in the Chinese mainland - “The Great Cyber Wall of China”, as it has aptly been called. Those ‘public’ hostile acts of a China awakening, when put together with Hillary Clinton’s, Robert Gates’, and even Barack Obama’s harsh rejoinders, plainly calling the Beijing authorities to account, clearly bring to the fore the ever more widely shared perception of the growing strategic centrality and scope of something that began as mere tactics of circumscribed convenience.

We soon will understand the range and import of the innovations, nevertheless, as both the Chinese loud operations and the US very public responses should - and surely will - be supplemented by a wave of thorough studies of the dynamics of the new matches being played. In this and numerous other cases, a novel game is indeed afoot, and most probably such ‘battle scenarios’ are here to stay.

Between a definition and a circumscription:
is there an emergent new template
for 'cyberwarfare'?

Cyberwarfare' is far more than a mere instrumental thing, comparable to, say, 'gun warfare', or 'tank warfare'. It is closer to things like 'psychwarfare', or even 'armed combat'. Perhaps mostly, it is much like "insurrectionary war"[7]. I mentioned that the action was "hybrid", and not in the purely "combined arms" sense - which will now likely always include cyberwarfare and underline the role of *civilian* participation in the conduction of hostilities.

Empirical data indeed suggests 'cyber-warriors' increasingly makes use of spontaneous civil society *compagnons de route*, even though it should be stressed at the very outset that this association still has a long way to go to become a fully-fledged canon in any meaningful sense. Can this be interpreted as an emerging doctrine or a contextual way to leverage 'cyber-anarchists' - the flocks of "hacktivists" - and sympathizers? Maybe this should be formulated in another way: how can civil society make itself an instrument of cyberpolitics**?** Is this an inevitable outcome of the growing virtualization of life, social relations and "hollow States" - as John Robb[8] **so graphically** put it?

Whatever our preferred answer may be, it is probably safe to stress that a doctrine of sorts is indeed crystallizing around a loose pattern of force-mobilization that we would be hard pressed to not recognize as growing very fast indeed - and this all over the world. The "hybridity" I mentioned will most certainly be there for as long as easy access, fast communication, and constant connectedness remains, empowering non-State actors all the way down to individuals - and perhaps beyond, to fashions, moods and states of mind. In virtual space too, free-lance participation in wars is becoming a parcel of the privatization of warfare - as a kind of *spontaneous outsourcing*. This trend will almost surely grow. 'Digital citizenship', as it has been called, is bound to intensify its expression in war, thus blurring even further the already less-than-neat traditional distinction between peaceful political mobilization and its many more agonistic variants - and it does so by rendering them all into manifestations of a more basic form of what I would be tempted to call 'asymmetrical resistance' to effective hierarchical power.

Ultimately, it is not difficult to see how and why this is so. Technology, for quite a long time, tended to favour the consolidation of political hierarchies. Modern technology, instead, largely because of its low cost and very low cost-steepness, appears to favor political decentralization by virtually universalizing empowerment. Computerized technologies also allow us greater degrees of technological integration across several domains as the use of digital technologies and multimedia allows a more fluid horizontal

integration among the actors. The key fact is that this integration is accessible - and with low costs - to almost anyone, albeit in different degrees of sophistication.

On the other hand, however, States and other 'nodal' hierarchical systems, no matter how much they are being "hollowed", to use Robb's expression, do not seem to be about to disappear; although threatened they will surely be capable of putting up a long effective fight for survival. So I surely am of the opinion we are into grass-roots empowerment for the long haul. In a very strong sense - and if new technological developments do not 'des-invent' such grass-roots force-gathering propensities, and of course they will not, or it is at least hard to see how they could - hybridity of the sort that one witnesses today in cyberwarfare (or even in plain participation in non-military active political movements) is here to stay. Many of the coordinates of our classical political landscapes - of the very topography of politics, really - are undergoing non-trivial changes. Such profound changes are often sensed by all of us, albeit often inchoately - and violent politics are particularly sensitive to these shifts. So this is a deep reconfiguration that we must learn to understand.

For the moment, we do not, not fully. Perhaps most interesting is the fact that the tactical entrance into scene of digital media quickly acquired clear and important strategic dimensions in a contemporary world embedded in an as far-reaching Information Revolution as the one we are zooming through.

Technical constrictions and the broad forms of political participation and association encouraged by different means of digital communication

We may and should dig further into this, as I believe we may gain from a series of complementary considerations which will allow us to unveil the emergent social dynamics of violent politics - and thus to act upon them.

In order to do so let me first latch onto the emergence of new communication technologies - and, in particular, onto their singular political impacts. I have no doubts that, at this level, what one notices most clearly and generically in what concerns new digital means of communication is the fascinating sort of *thickening of political participation* they tend to engender - a participation which is enormously amplified by the mere existence of such networks. Moreover, besides this intensification one witnesses a change: the political participation we see is both more spontaneous and expressed in new

formats - and these are often design layouts which deeply reconfigure its political mechanics. This is of course something that cannot but deeply affect the inner mechanism of the budding realities of cyberwarfare - and something we can perhaps use to our advantage.

Let us focus, in a first step, on this reconfiguration of the internal workings of political participation actually engendered by new communication technologies. In order to see this, it should be enough to focus, if only for a brief moment, on one example only: that of the so-called social networks - so allow me to do just that. While I have my own view on the subject, I draw on numerous and very good studies on the complex dynamics of these novel entities which were carried out by the likes of Danah Boyd, Yochai Benkler[9] Anne-Marie Slaughter, or Jack Balkin, the first two in Harvard, the last couple, respectively, at Princeton and at Yale. The crux is: *do different social communication network technologies give rise to different political modalities of participation, association, and action*?

It is surely simpler to begin by looking at such impacts in general terms - outside any reference to their use in warfare. Not going further than scratching the surface at present, we may begin by noting that the types of sociability generated, or segregated, by these social networks, albeit largely spontaneous, are rather distinct and clear-cut. Awareness of this, crops up, rather straightforwardly, from the evidence that the scale and scopes of such forms of sociability are huge, their growth fast, and their innovative strains astounding - and that the self-organizing mechanisms of these new emergent virtual communities often become paramount.

How and why? Polarizing a trifle and simplifying as if by compression, so to speak - a rich discussion, and surely one which deserves far more attention than it has received - it is maybe not excessive to point out two polar positions held by analysts about such topics. One of them claims these networks are themselves simple instruments, mere vehicles, of earlier political intentions, values, and wills; that they are thus permeated by an ethic, and that therefore they do not in any relevant sense format any sort of “new” politics at all. But there is another take that follows the opposite tack: one which insists, instead, that “the medium is somehow effectively the message”; that it is indeed so in a quite strong manner - and, therefore, that there are structural traits of networks that very effectively pattern the political participation of those who use them. This last vein seems to be the most convincing one, although this is of course arguable. Thus, I do consider the very *sui generis* pattern of sociability - ‘civility’ might be a better term, here - which flows from the structural traits of communications media, in our case, *virtual social* media, to have a significant political impact on both group formation and potential contours of political participation.

Such a rise of new political formats happens, simultaneously, from the perspective of the network's topology, with organizational shapes and potentials coming up, on the one hand; and, on the other hand, from the perspective of the political will of participants - those who coalesce in them, and whose "subjectivity" is thereby built according to very specific mechanisms. From the angle of their will, or of their disposition to participate, those who do gather do indeed structure what Donald Rumsfeld would perhaps have called *coalitions of the digitally willing*: expressions of 'opportunistic' entities which, of their own accord, decide to participate in the novel and emergent network. From the perspective of the logic of the network itself, they as if coagulate into "affinity groupings" [an anarcho-syndicalist term]: new collective formats emerge which, step by step - and responding to those wills - fast or slowly crystallize.

Such political forms are indeed here, of that there can be no doubt. With digital social networks, we witness the appearance, in our contemporary stages, of groupings and activities of a new sort - ones in which people only participate out of their choice to do so and according to common denominators they feel unite them for the purpose. It seems clear too that a network which depends on an affinity group and then mobilizes persons so that they will feel a desire to be moved by the "cause", or the causes, it spells - the common denominator that 'gestates' it - cannot but constitute an instrument which patterns - and does so *ab initio* - from a political angle, the very *structural* nature, or essence, of the effective political participation this network - in a full sense - *produces*.

In other words, potential (but rather tangible) political implications, somehow indexed on the network's structure, are indeed easily associated with that spontaneity. By giving a few examples, I now want to dig into this very point of the different "political communities" produced by different digital networks, and the diverse "modes of subjectivation" which are the net outcome of their use - so that further down the road I shall be able to link such issues to the varying topologies of cybernetic space and to the implication this in turn spells as far as the geopolitics of those new virtual spaces is concerned.

What, then, are some of the most significant differences in personal and communicational patternings which flow out of political participation in those networks? What is their political structure, in other words? There are quite a few differences at that level, as we shall see - and such differences, as I will try to make clear, are in fact rooted in a variety of complementary planes.

Again, allow me to tackle the matter in a rather neutral and abstract way, with nothing but general allusions to agonistic politics. On a first approach, it should be noted that the various different types of political participation witnessed are ordered in terms of alternative logics - and that these are in turn entrenched, *grosso modo*, in different technological "generations" of social networks. Notice, for instance, how changes are

sequentially, but not in any meaningful sense cumulatively, ordered along a time axis. A handful of examples: there are now few Western countries in which Hi5 (much like MySpace) is still stoutly on the rise - and notice that Hi5 is not as *interactive* a social network as the more recent ones, as it is mostly *passive*; what we have here is a sort of "store window" where pictures of pretty girls and available boys are hung - or a place of "people like us"; with a completely different purpose, the same is true of Linkedin. Hi5 is indeed a bit like a virtual phonebook - a particularly rich one, as it contains far more information (namely visual information) than is usual in any kind of phone lists. Then came Facebook, a much more recent entity, a new generation network - and it fast turned into a medium, whose users are mostly people between 25 and 50[10]. Diacritical differences between these two generations of social networks abound. It would not be an exaggeration to claim that Facebook is a high-tech kind of enlarged family album (sometimes drifting into a sort of modern Tupperware party). Albeit a mere 'aggregate collection', one that does erect a web of friendships that is surely much more interactive than that brought up by the oldish Hi5 - but much less so than, say, Twitter, a third-generation entity insofar as ideational-technological innovations go.

With Twitter, broadcasting widely what I am doing at any one moment, sharing in real-time what I am actually carrying out at a given point in time, is the central task of the network. What becomes segregated as a result, are neither "buyer friends" - leaning over the store-window, in a listing similar to that of Hi5 - nor real "sympathizers" in a full sense, as in Facebook or in Friendster. With Twitter, "followers" are spawned, instead, "disciples", in a curiously subaltern sense - the "immediacy" of its "real-time" flows of emission-reception probably enhancing that gap. The web created by Twitter mobilizes follower-disciples in a rather curious manner, one which flows largely from the technical conditions built into its operation as a communicational device. To put it perhaps too bluntly: up against a maximum limit of 140 characters I can only *tactically* mobilize any followers, as I may only draw on short and simple *mots d'ordre* - by issuing commands such as "turn right!", or "withdraw now, they are moving in on your position!", much like in a military operation, or in, say, a public demonstration in Teheran, by announcing loudly the presence of *basij* militias or hitmen on Mainstreet X, as Twitter was indeed used in Iran in June 2009. I shall return to this very point.

On Facebook, matters are not quite the same, given the design of its support and the type of communication and interaction it both allows and stimulates: Facebook, of course, permits much more complex strategic manoeuvers - and therefore different types of political community may be indexed in very different organizational structures when their gestation is a upshot of this other digital social network. With Facebook we are indeed capable of sketching what we normally call a "doctrine" - something which with Twitter is well-nigh impossible. If with Twitter, in other words, we may merely give instructions and issue commands; with Facebook we are capable of delineating drafts of I am tempted to call "cosmologies" - programmatic agendas, if you will. And that makes all the difference: if, in the Twitter case, we are stuck with flashes, with Facebook we are capable of

breeding coherent - and often fairly elaborate - world-views. In yet other words, as they stand, the features of Twitter make it especially adequate for "tactical moves" and for basic efforts of "*recruitment* and 'direct action' *mobilization*"[11]. Facebook, on the other hand, may be a good template for the sorts of social software useful in the building of "strategic-support *stands*" rendering it possible, for example, to put together, via, say, a wiki toolset, new "decentralized" *theories* - political or other.

The contours of political action stimulated by different digital means of communication and their use in conflicts

I believe I have shown they are of course not something we can easily discard as politically irrelevant. Both negatively and positively, different digital communication modes do tend to rouse and promote different group formats and profiles. Now, in what precise sense do technological constraints bear on the political 'tactical and strategic texturing' of cyberspace conflicts? Further resolving images by comparing the functioning of communicational platforms in conflict situations and pondering over their political implications in agonistic contexts - even if only lightly - is a useful step for delineating a more detailed answer.

To enounce things crisply: what are the built-in biases, what is the *range* of the political repercussions of these diacritical differences - and, perhaps crucially for our discussion here, how does all this relate to cyberwarfare? To offer an answer to this, let us now briefly seek for details of the inner linkage between structural form and political mechanics - this, in turn, brings us closer to home, *the political architecture of cyberspace*.

We may note, first, that as suggested earlier, dissimilarities in technological constraints both help give rise to *different types of groupings* and tend to shove them into quite *distinctive political dynamics*. Second, we may stress the evidence that some of the types of groups formed tend to spread by 'metastases' more than others - and that, in the process, some of the types of groups fostered 'mutate' more and faster too. I.e., different forms of political association spawned by different digital communication devices *both act and metamorphose differently*.

Two examples should suffice as illustrative paradigmatic cases: the disparate patterns and dynamics of Facebook and Twitter generated groups already sketched out. As suggested –and as all users of Facebook are surely alert to - this social networking tool is

particularly apt for drawing “petitions” and for the development of “advocacy groups”. Moreover, as underlined, as a response to Facebook’s traits these typically aggregate around pressing but comparatively timeless and ‘doctrinal’ matters. We should dissect this insight a little by looking into the actual workings of the groupings formed. Throughout 2009, for instance, a variety of texts were submitted and subscribed by Facebook users on issues ranging from opposition to the death penalty in the US and elsewhere to animal abuse in China to appeals to the protection of national agricultural products, and/or to the mobilization of support networks of citizens concerned with the revival of anti-Semitism - or of others loudly appealing for gay marriage or protecting the right to life. Facebook is typically littered with calls for groups to coalesce around such political mainstream-style ‘causes’ on par with others aimed instead at pushing for the creation of cliques of support for particular Nobel candidacies or the formation of posthumous Michael Jackson fan clubs.

Interestingly, these conglomerates of cause-followers tend to be rather static entities, ones which form so as to be function as classical pressure groups. When the Spring 2009 protests began in Teheran, a variety of Facebook pages grew so as to mobilize people for a staunch defense of Human Rights in Iran - as well as quite a few keen on transforming Neda Agha Soltan as a symbol and martyr for the uprising and the struggle against the oppressive ayatollah regime. In these as in most cases, such Facebook ‘causes’ aim at displaying to the powers-that-be the presence of public programmatic opposition (or of support) for ‘*significant*’ and *structural* matters. Rarely do they center attention on daily ‘real-time’ day-to-day issues unless they do so quite revealingly tongue-in-cheek - say by appealing to the creation of groups opposed to John Smith’s choice of silk ties, or by calling for a much needed support to the Society for the Protection of the Rights of Swedish Underwear Models.

Twitter-generated groups and movements, on the other hand, as I underlined, are different –and much more event-focused - in their *modus operandi*. Relevant streams of tweets were usefully sent from mobile phones as the dramatic events took place during and after the May 2008 earthquake in China, as they were handy during the forced water-landing of a US Airways aircraft in the Hudson River, in Manhattan, in May 2009. Their aim was far more pragmatic and action-driven - and as information flowed, groups coalesced. Politically, so to speak, tweets also were instrumental, in that very same month of May 2009, in Moldova, when coupled to protests against the highly irregular elections which returned the communists to power in Chisinau; or in Guatemala, in massive demonstrations against a President, Álvaro Colom, blamed of orchestrating, a day earlier, the murder of an opposition journalist who had accused the Guatemalan Head of State of corruption - as has often been the pattern, an event first broadcast in YouTube and then given wide publicity via Twitter.

Comparisons bring home clearly the core traits of these Facebook-style sociopolitical processes: in a case I earlier mentioned - and so as to elude authorities - young Iranians

in mid-2009 resorted to a free open-source piece of software appropriately called *Freegate*. This was written by US-based Chinese engineers in order to help Falun Gong, a spiritual group harshly persecuted by Beijing's authorities. To escape government censorship, the program, housed in a drive, directs Internet navigators to an external server which changes their IP addresses once every second - way too fast, of course, for censors to be capable of 'reacting'. *Freegate* was made widely available in Farsi in 2008 and, not surprisingly, it grew exponentially in Iran - a country whose youth has no memory of the Shah or of the coup that took him down in 1979, and who developed one of the world's most vibrant blogger communities.

It should be clear by now, I hope, how all this connects to cyberwarfare and its 'social-political' dimensions - namely about the special 'texturing' of the hybridity it displays and its roots and repercussions. They tie quite a bit, I would argue, and rather linearly: events show us that tactical and 'doctrinal' hacktivist mobs alike are often simultaneous parcels of contemporary hybrid cyberwarring.

Instead of detailing here and now some these obvious links - which would amount to a new paper - I want to draw this segment to a close by going back to an earlier point I made. New communication technologies are becoming more and more pervasive in all spans of life today. True enough, such profuse messaging is nowadays becoming as if diluted in the thick flow. Messages are de-centered and fragmented, for sure - as we know, tweets only bear a minimal density of information. Most relevant, however, is the evidence that *robust messages* emanating from a central point - say, 'bodies of political doctrine' - no longer have a monopoly on public political discourse. New centers for 'doctrinal production' are emerging. The new digital technologies which are all around us, it should be highlighted, are thus latent revolutionary tools - and they are so in the very measure that they do take away from any groups (say, States) their traditional monopoly on public political discourses, redistributing discursive production to all interested and 'connected' social entities and segments.

Moreover, such technologies, I want to again underscore, are potentially revolutionary *in themselves* - since, if up until now communication technologies have systematically centralization, modern digital developments awaken and ignite, instead, political decentralization[12]. To be sure, these technologies are amenable to use as both instruments of political control and as parallel tools of subversion; that is, they can, at once, give rise to hitherto unimaginably centralized mechanisms for political control and means for toppling them. With States and non-State actors increasingly resorting to virtual chat-rooms, blogs, and a variety of types of instant messaging in the conduct of conflicts, obviously wars constitute no exception to such trends, as recent events have come to show us - the cyberattacks on Georgian targets in August 2008 which I roughly described were a clear-cut example of such novel political features.

Before moving on to grander questions concerning the emergent topographies of hybrid warfare, a few comments on our levels of readiness for successfully standing up to it seem apposite.

Fragmentary levels of preparedness

NATO and the US - much less so the European Union, as could be expected[13] - have begun to pay some attention to these dynamics. Not all action has to come from State agencies, so non-traditional players (non-State actors, even networked and bored adolescents) may be disruptive. How can national and international agencies deal with this? The short answer is they cannot, not in the mid- and long term. But as a short term solution they can and they do indeed try to methodically deal with the disruptive effect of those "dynamics". How so? Well, here goes a short answer, in which I shall argue States are capable of doing this in two complementary ways.

National and international agencies can forestall disruption by either going 'networky' themselves, and/or by selective counter-strikes. I do not want to go into this in very great detail, but I would nevertheless like to give a few pointers here. For the first tactical move - 'going networky' as an adaptive response, in a sort of arms race - much has been written. Look up, for example, Anne-Marie Slaughter's work at Princeton or Yochai Benkler's at Harvard, as earlier mentioned - hers on the growth of networked political, administrative and legal structures, his mostly on the latter. By doing that, States and international organizations (a) become more resilient themselves, and, (b) their increased agility sometimes allows them to disrupt the disruptors. The thing to underline here is that if, on the one hand, States and State-centered entities (and this is what most international organizations actually are in our Westphalian world) must act as if *contra natura* in order to go networked, on the other hand they surely have the means to do that - at least temporarily, in a Weberian vein - with relative ease.

In order to see clearly that this works, we ought to reason by exclusion. As an example, simply ask yourself the question: if networks do indeed have such an immense set of advantages when confronting hierarchies, how come al-Qaeda terrorists, for instance, do not win clashes against them *every time*? The answer is simple: in spite of their comparative structural disadvantages, the raw fact is States have many more resources at their disposal than do terrorist networks. Besides, the cost of failures is disproportionate: al-Qaeda can achieve its goal even through failed attacks, by inducing terror and creating disruptions in the target's infrastructure. Indeed, failed attacks - and especially suicide attacks - allow the perpetrator to stay alive, which translates into a

highly efficient cost-benefit ratio. And segregating anti-network networks has often served States well - as may be seen with entities like Homeland Security, the UN, the institution of diplomacy, or the new military doctrine of “swarming”, States are even capable of generating mid- to short-lived networks when the need arises, to do work they themselves cannot *directly* carry out.

In the second place, States can forestall immediate disruption at the hands of digitally viable ‘wired’ networks by engaging in precisely targeted selective counter-strikes. Experience shows that when States and multilateral military alliances do this swiftly enough, and in a well-calibrated rhythm, they do manage to quite effectively slow ‘malicious’ external network-induced cascades. Here they must bring to bear their vastly superior means. This has been taking place in many fronts, although it may come as a surprise to note that, apparently, in what concerns political-military disruption, for all of Washington’s dominant place in the Alliance, NATO has not in fact acted in the wake of the US, things have in fact mostly gone the other way round. In other words, NATO is often more agile than the US itself… While this is not the case across the board, that this is largely true in what concerns many general cybersecurity issues cannot be doubted. Let me give you just one example among many possible ones - and it will be the reaction of NATO and the US to cyberwarfare itself. Following the Spring 2007 waves of systematic attacks of Russian origin on a huge number of Tallinn official Internet servers, NATO created a cyberwarfare ‘Center of Excellence’[14] there. It was from whence that came many of the specialists called into Georgia in August 2008, following the concerted ground, aerial, and naval attacks launched from Russia and Ukrainian Crimea in rather close synch with the invasion of South Ossetia and Abkhazia ordered by the Kremlin.

NATO, then, seems to be moving up to speed, as far as cybersecurity is concerned. What about the US? Allow me to quote at some length from the wonderful *Amitai Etzioni Notes* weblog, and specifically from the 11th June 2009 blog entry: “several major security threats […] were largely ignored by the Bush-Cheney Administration. [Now] it is the Obama Administration that is attending to these threats, and in ways that progressive people have little reason to oppose. The threats include, first of all, the dangers posed by cyber terrorists to both the government and the private sector. Given the way U.S. computer networks are now exposed, little information - whether it concerns security or the economy - can be kept confidential. Moreover, cyber attacks can readily disrupt key elements of US infrastructure, such as air traffic. In 2008, hackers breached government computers and planted harmful software 5,499 times. Cyber spies stole information on the Defense Department’s Joint Strike Fighter. It was left to Barack Obama to pay the proper attention that this issue commands by appointing a cyber security czar, a long overdue step in the right direction. Equally exposed is the electrical grid on which U.S. factories, offices and homes all rely. Software programs were found to have been planted in the U.S. electrical grid that could be used to disrupt the system in the future. An experiment in an Idaho demonstrated that hackers could command an electricity-producing turbine to spin in ways that would cause it to fly apart. Another security

matter the previous administration did not address". Not so good... It seems that, if anything, the US Administration is crawling in the wake of NATO[15]. As, indeed, is the European Union - although that surely comes as a lesser surprise. But after six years of cyber-tension the wakeup calls worked: on the 1st October 2009, a Cyber Command (USCYBERCOM) was formally created by Washington, headed by a recently Senate-confirmed four-star General, Keith Alexander, the Head of NSA and with a man-power of two hundred and forty thousand men and women[16]. The new game is indeed afoot.

Is the EU playing the game too? Somehow, yes. A sketchy picture: it was only in the last few months of 2009 that the EU's newly-created 'cyber security' Agency ENISA, i.e. the European Network and Information Security Agency, received its new Executive Director - as of 16th October, the position was taken by Dr Udo Helmbrecht. Dr Helmbrecht is the former President of the German IT Security Agency BSI, the Federal Office for Information Security. Let us see how it fares.

Are we drifting toward a disparate and asymmetrical, and both material and virtual, security future - and a new waxing and waning of geopolitics?

Can we generalize? With the aim of widening our scope, and as a sort of closing gambit, I want to jump ahead of the main thrust of my central geostrategic considerations. I will begin doing so by bringing up a political aspect of the sorts of innovations we confront, one which follows from the well-known and often discussed contemporary increase in surveillance politics - in this case in connection with State responses to the growing efficacy of 'private' and 'wired' political actors in an increasingly globalized environment marked more than ever by complex and thick interdependences of all sorts. I shall then move on to wider scenarios.

Networking is now widespread, and this makes it ever more patent that a 'virtual international civil society', even if it is yet a brittle and not very robust entity, is coalescing and gaining weight and self-awareness. In the digital world too, an international society is indeed forming. Faced with contentious experiences, international public opinion, virtual and 'material', flares up - and al-Qaedas are instantiations of that. Understandably, States have reacted to the perceived and often very real threats they pose by repression and increased surveillance. To focus just on this last response: without a doubt there is the possibility that surveillance and 'negative liberty' - freedom from interference by other people - as, after Hobbes, Isaiah Berlin called it, fall out of step with each other; in fact, even if many of us are blissfully unaware of it, that inability

for keeping pace is already hampering things.

There are a couple of good reasons, at least, why that is not barefacedly blatant to all of us. One is connected to the fact that the general surveillance to which we are increasingly subjected is by no means as publicized and acknowledged as it undoubtedly should be. Another cause for the relative invisibility of this out-of-stepness is linked to the very fast increase in surveillance which followed 9/11 - a surge which sort of hid its structural decrease in efficacy[17]. In other words, surveillance is on the rise, and that may be a threat, but that is only half the story. Since the technology (malware, viruses, Trojans, DDoS**,** etc.) to neutralize such State moves is so widespread and 'public', is there not the risk that 'public surveillance' cannot keep pace with these smaller and more dynamic actors? Indeed, States are oftentimes losing the battle: one can easily see the inabilities of surveillance in keeping pace with the decentralizing political empowerment effects of digital technologies at work through the refraction of the frantic, and largely unsuccessful, rear-guard attempts to uphold the old intellectual property laws. Small, modular, agile groupings slip through the fingers of slow-moving heavy hierarchical systems - in spite of their logistical robustness, States and big corporations are often simply not capable of keeping up with these novel and more dynamic actors to whom digital technologies bestow power - and, let me insist, were it not for the very tangible reinforcement of effective surveillance following 9/11 we would all immediately see how much that is increasingly the case. True, the succesful countering of demonstrators, often violent ones, at the June 2010 meetings of the G-20 Summit in Toronto, Canada, does show some level of effective organizational learning by ever more supple and nimble security forces miming such contemporary adversaries. But States can no longer be sure that they still hold the upper hand. So risks increase.

Now, given the unbalance of costs and effects in cyberwarfare, and taking into account the participatory lures it offers to us as 'digital citizens', will cyberattacks become a mainstay in politics for the 21st century, either as a new form of "war" or just as plain old "politics by other means"? My bet goes for staple mainstay. Notwithstanding voices to the contrary, I do not believe we are witnessing - or even that it is likely we shall be faced with - an entirely new kind of "war". True, the conjuncture is altered, in a deep structural sense. Indeed, new political landscapes mean that "politics by other means" will be rather different from the run-of-the-mill affairs. It is not just a question of means, of the seditious potentials of the new formats of empowerment. Motives are not lacking either: the asymmetries, e.g., are far greater now than at any time since the early 50s. Moreover, complex interdependence is thicker than ever: we call it globalization, nowadays, even *la mondialisation* - and in our ever more connected and transparent global village, exclusions are there for all to see.

This patterns cyberspace in a significant way - and that, in turn, gives it specific political properties which crisply come to the fore as soon as conflicts arise. But it would be excessive to think we are eyewitnesses and participants in a radical break with the past,

for the ongoing changes hide a long-term set of continuities, ones which may perhaps be portrayed as follows: it does not really matter what the novel specifics properties and potential unfolding of cyberspace amount to as far as wars are concerned - for ultimately cybersecurity is hardly more than a new dimensionalization of 'geopolitical' space, even if it does blur the boundaries between 'normal' and so-called 'virtual' space.

That should nevertheless give us no pause, for as new thresholds are reached large quantitative alterations do eventually transmute into qualitative ones, so the politics of conflicts in cyberspace will not be the same as those of old ones - thus the change we are witnessing in the last decade or so will lead to a rejuvenation of politics, and surely deep changes in agonistic forms of politics. It is precisely at this level - that of *the social politics of combat* - that I believe most significant novelties will crop up. We do not know what that shall be, but I am confident those new politics of combat will bear a closer resemblance to "insurrectionary war" than to "class warfare". Also, in a communicative world, "motives" may well become stronger than "interests" - although it would of course be difficult to argue all these are not mutually reinforcing trends.

Thus, notwithstanding the foreseeable supremacy of States for a long time to come, the shifts in power which the rise of this architecture called cyberspace creates will have non-trivial geopolitical correlates - some of which I have mapped out. Does this tell us anything relevant? Namely, does it give us useful hints on how to fight these new types of war? It tells us that when faced with swarms of malevolent "hacktivists" we should ask questions such as "what is the patterning of communications shaping the 'mob' involved in this particular cyberattack", "what tactics should be expected from this particular mob-type", or "what changes are we capable of inducing into the political profile of the 'mob' engaged in the cyberattack, and how do we trigger those". Knowing the shape of communications and thus the internal political dynamics of the active groupings will often give us useful clues on how to change their modes of operation by developing carefully designed and well-calibrated ripostes to their *modi operandi*.

Should we then not attempt to make an educated guess as to what we shall witness in this cyberspace which re-dimensions war and geopolitics? Indeed, is it not our political and ethical obligation to do so, if only as part of a generational compact? I want to connect this to what I said before. As new digital communication technologies empower us, they do so both bottom-up and top-down; moreover, their coming into play can have 'liberative' as well as repressive outcomes. Our quandary is all this happens simultaneously, and the battle is far from over - since rather than mere inert instruments of processes of self-construction, these technologies form an integral part of the social and political ecosystem which fundamentally builds our feelings of 'me', 'us', and 'them', by outlining and molding our surroundings, relationships, dealings, and affairs. Like all communication, the new more inclusive digital one is not just something with which we live: it is constitutive of our very identities. All our social and political relationships - including hostility and war - are now embedded in these new forms of communication and

every day further permeated by them. A multi-dimensional sort of identity layering (or an intrinsic complexity in what amounts to a multi-level production of subjectivity, if you will) is patently cropping up and it is one which makes all the difference: one that splits feelings of 'belonging' and ties of loyalty too. I would not be surprised if a multi-dimensional sort of "neo-medievalism"[18] settled down on us.

The hybridism of emergent cyberwarfare, I want to argue, ultimately has its roots in this very foundational nexus. My guess is that after the brief 'modernist' spell begun in the late 18th Century and is perhaps quickly closing we will go 'conventional' again - back to multidimensional identity construction and layered loyalties, or multi-level ones, something which has for so long constituted what we learned to call *la condition humaine*. Each and all of us can be many in one. The social politics of conflicts will increasingly mirror this. Innovative hacktivist mobs will form, in ever more inventive political shapes. New modalities of rationality will emerge. Tomorrow shall not be like today.

Bibliography

Anders Albrechtslund (2008), "Online Social Networking as Participatory Surveillance", First Monday, volume 13, number 3, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949

Anne-Marie Slaughter (2004), *A New World Order*, Princeton University Press.

Armando Marques Guedes (2009), *A Guerra dos Cinco Dias. A Invasão da Geórgia pela Federação Russa*, Instituto de Estudos Superiores Militares e Prefácio, Ministério da Defesa, Lisboa.

_____ (2010), "Geopolitica del Ciberspazio", in the last *Quaderni Speciali di Limes*. *Rivista Italiana di Geopolitica*: 187-199, Roma.

CSIS Commission on CyberSecurity for the 44th Presidency (2008), "Securing Cyberspace for the 44th Presidency", available for download at http://csis.org/files/media/csis/pubs/081208securingcyberspace44.pdf.

Congressional Research Service (2009), Comprehensive National Cybersecurity Initiative: Legal Authority and Policy Considerations, available at http://assets.opencrs.com/rpts/R40427_20090310.pdf.

danah boyd (2008), "Can Social Networking Sites Enable Political Action?", in (eds.) Allison Fine, Micah Sifry, Andrew Rasiej and Josh Levy, *Rebooting America:* 114, Creative Commons.

Gadi Evron (2008), "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War", *Georgetown Journal of International Affairs*, available at http://ciaonet.org/journals/gjia/v9i1/0000699.pdf.

Government of Georgia (2009), *Russian Invasion of Georgia*. *Russian Cyberwar on*

Georgia,available at http://hostexploit.com/downloads/CYBERWAR%20fd_2_new.pdf
Greg Bruno (2008), *The Evolution of Cyber Warfare*, The Council on Foreign Relations, available at http://www.cfr.org/publication/15577/.
Hedley Bull (1977), *The Anarchical Society. A study of order in world politics*, MacMillan, London.
Jack Balkin and Beth Noveck (2006), *The State of Play: Law, Games and Virtual Worlds*, New York University Press.
John Robb (2007), *Brave New War: The Next Stage of Terrorism and the End of Globalization*, Wiley. See also http://globalguerrillas.typepad.com/about.html.
John S. Monroe (2009), "Cyber Command: So much still to know", *Federal Computer Week*, available in http://www.fcw.com/Articles/2009/07/06/buzz-cyber-command.aspx.
Nick Farrell (October 2008), "Russia not responsible for cyber war on Georgia", *ITExamminer.com*.
Ronald Deibert and Rafal Rohozinski (2008), "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet", in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press, available at http://opennet.net/accessdenied.
Yochai Benkler (2006), *The Wealth of Networks, how social production transforms markets and freedom*, Yale University Press.

---

* Estudou Administração Política no Instituto Superior de Ciências Sociais e Políticas (ISCSP), *Social Anthropology* na *London School of Economics and Political Science* (LSE), com um BSc (Honours) e um MPhil, e com um Diplôme em *Anthropologie Sociale* na *École des Hautes Études en Sciences Sociales* (EHESS), em Paris. Doutorou-se em Antropologia Social e Cultural na Faculdade de Ciências Sociais e Humanas (FCSH), Universidade Nova de Lisboa. Agregou-se em Direito na Faculdade de Direito da Universidade Nova de Lisboa (FDUNL). É Professor Associado com Agregação, de nomeação definitiva, desta última, do Instituto de Estudos Superiores Militares (IESM), Ministério da Defesa, e do Instituto de Ciências Policiais e Segurança Interna (ISCPSI), Ministério da Administração Interna. Entre outras posições, foi o primeiro Conselheiro Cultural da Embaixada de Portugal em Luanda, entre 1985 e 1990, de 2005 a 2008 foi Presidente do Instituto Diplomático, no Ministério dos Negócios Estrangeiros português e Director de *Policy Planning* no mesmo. Proferiu Conferências e palestras e/ou organizou Cursos em mais de quatro dezenas de países. É autor de quinze livros e mais de setenta artigos e membro de uma vintena de Sociedades científicas, em Portugal e no estrangeiro.

[1]Even though, for reasons of inclusiveness linked to my intention to continue working on these and other akin subject-matters, I include the word "geopolitical" in my title, the

present study is mostly in actual fact concerned with geostrategy and some of its new operational dimensions. An article of mine, in Italian, which develops a set of arguments rather similar to the ones expounded here, was published under the title "Geopolitica del Ciberspazio", in the last *Quaderni Speciali di Limes*. *Rivista Italiana di Geopolitica*: 187-199, Roma, that came out in June 2010. Although with a few small but somewhat significant changes, the present paper follows closely what I then wrote.

[2] I discuss this and more in a work published by the Portuguese Institute for Higher Military Studies (IESM): Armando Marques Guedes (2009), *A Guerra dos Cinco Dias. A Invasão da Geórgia pela Federação Russa*, Instituto de Estudos Superiores Militares e Prefácio, Ministério da Defesa, Lisboa. One of its sections is on 'Moscow's' cyberwar against Tbilisi.

[3] The Report is available at http://hostexploit.com/downloads/CYBERWAR%20fd_2_new.pdf

[4] Nick Farrell (October 2008), "Russia not responsible for cyber war on Georgia", *ITExamminer.com*.

[5] In a rich blog which goes far beyond simple matters of war or technology, found at http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html?nav=rss_blog.

[6] Maybe we should use the term 'cooperation' or even 'commensalism' along with 'parasitism', since both "parties" (or types of participants) benefited from their temporary convergence of objectives - or, at the very least, actions.

[7] For an overview, see Greg Bruno (2008), *The Evolution of Cyber Warfare*, The Council on Foreign Relations, available at http://www.cfr.org/publication/15577/. For a good study on the tactics used (denial of access through server-control) read Ronald Deibert and Rafal Rohozinski (2008), "Good for Liberty, Bad for Security? Global Civil Society and the Securitization of the Internet", in Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain (eds.), *Access Denied: The Practice and Policy of Global Internet Filtering*, Cambridge: MIT Press, available at http://opennet.net/accessdenied.

[8] In John Robb (2007), *Brave New War: The Next Stage of Terrorism and the End of Globalization*, Wiley. See also http://globalguerrillas.typepad.com/about.html

[9] Danah Boyd [or danah boyd, as she writes her own name] has far too many small articles on "sociality" and the "culture and politics" of social networks for me to list here, ranging from studies on the specifics 'properties' of Facebook, Twitter, MySpace, or Friendster, to the explosive growth of both "teen and adult networked publics". For an ambitious study on the new economics and politics of the Information Revolution, see the authoritative Yochai Benkler (2006), *The Wealth of Networks, how social production transforms markets and freedom*, Yale University Press. Anne-Marie Slaughter's classic, her 2004, *A New World Order*, Princeton University Press, focuses on the increasingly networked legal and judicial systems of contemporary "disaggregated States". Jack Balkin's most relevant work is perhaps is monumental 2006 *The State of Play: Law, Games and Virtual Worlds*, New York University Press, written with Beth Noveck. Relevant articles by these authors may be found at www.danah.org/papers/, www.benkler.org,www.primceton.edu/~slaughtr/publications.html, and www.yale.edu/lawweb/jbalkin/balkbibl.htm. These are just a few major references in an

exploding field.
[10] Although these are changing demographics, some 80% of Facebook users fall, consistently, in this age bracket; see, for instance, http://www.fastcompany.com/magazine/115/open_features
-hacker-dropout-ceo-facebook-numbers.html. In 67% of users fall in the lower 18-34 age bracket:
http://francewebe-globalnewscenter.20minutes-blogs.fr/archive/2009/12/06/stefan
-raducanu-mynewscenter-hi5-millions-of-users-one-globa.html.
[11] To be sure, this is all changing fast: Twitter may now, even if only in a limited sense, originate something akin to classic "doctrines". A famous attempt, in 2009, to write a narrative via tweets (a theatrical play) largely failed. However, it might still be possible to draw "lines in the digital sand", as the application gathers momentum and becomes more open to other uses: it is now possible to create Twitter user lists, for example - something that did not exist six months ago. Embedding the stream of one user into a body composed of the tweets of a circumscribed group, the lists signal the rise of a community that establishes relationships based on affinity, common interests or even allowing users to "avoid" lists that draw semantic and symbolic lines. My point is of course analytical, not empirical.
[12] One example. "[t]elephones allow people to communicate over long distances. Activists know that the bullhorn of the Web lets them reach many more people, even in the context of a supposed shared space. The Internet not only collapses space and time, but beyond bandwidth, there is no additional structural cost between communicating with ten people and broadcasting to millions. danah boyd (2008), "Can Social Networking Sites Enable Political Action?", in (eds.) Allison Fine, Micah Sifry, Andrew Rasiej and Josh Levy, *Rebooting America:* 114, Creative Commons.
[13] It was only in the last few months of 2009 that the EU's newly-created 'cyber security' Agency ENISA, i.e. the European Network and Information Security Agency, received its new Executive Director - as of 16th October, the position was taken by Dr Udo Helmbrecht. Dr Helmbrecht is the former President of the German IT Security Agency BSI, the Federal Office for Information Security.
[14] NATO's aptly called *Cooperative Cyber Defence Centre of Excellence* (CCD COE) operates out of Tallinn, Estonia, since August 2008. Choosing Talinn was of course not accidental, as it was there that, in the spring of 2007, Estonian authorities moved a monument to the Red Army (the Bronze Soldier) from the center of their capital, Tallinn, to the outskirts of town. A diplomatic row erupted with neighboring Russia, and this was followed by massive cyberattacks and defacements of Estonian official servers and sites - parliament, Ministries, banks, political parties, etc.. For an analysis, see Gadi Evron (2008), "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War", *Georgetown Journal of International Affairs*, available at http://ciaonet.org/journals/gjia/v9i1/0000699.pdf. Fascinatingly, James Hendler, a former chief scientist at the Pentagon's *Defense Advanced Research Projects Agency* (DARPA) characterized the attacks as "more like a cyber riot than a military attack". Interestingly, Colonel Anatoly Tsyganok, then Head of Russian Military Forecasting Center, confirmed Russia's ability to conduct such an attack when he stated: "[t]hese attacks have been quite successful, and today the alliance [NATO] had nothing to oppose Russia's virtual

attacks". He followed these remarks with the claim there was nothing illegal, according to International Law, about the events.

[15] See the general overview of the CSIS Commission on CyberSecurity for the 44th Presidency. 2008. "Securing Cyberspace for the 44th Presidency", available for download at http://csis.org/files/media/csis/pubs/081208securingcyberspace44.pdf. See, also, Congressional Research Service (2009), Comprehensive National Cybersecurity Initiative: Legal Authority and Policy Considerations, available at http://assets.opencrs.com/rpts/R40427_20090310.pdf.

[16] See John S. Monroe (2009), "Cyber Command: So much still to know", *Federal Computer Week*, available in http://www.fcw.com/Articles/2009/07/06/buzz-cyber-command.aspx.

[17] This does not mean, of course, subtle surveillance modes are not on the rise. It just means surveillance must be rethought. Among other things, and this is too often overlooked, we must be aware that insidious and, in a sense, counter-intuitive, modes of surveillance seem to be creeping into our lives, hand in hand with bottom-up empowerment. One example of this is what Anders Albrechtslund called "participatory surveillance": the one provided by online social networking practices. Online social networking, as Albrechtslund stressed, offers us a splendid opportunity to "rethink" the very concept of surveillance - by somehow adding to it the possibilities of voluntary forms of this participatory surveillance, involving mutuality, empowerment and sharing. Benevolent forms of surveillance, so to speak, in the sense of forms non-inhibiting of negative freedom. Anders Albrechtslund (2008), "Online Social Networking as Participatory Surveillance", First Monday, volume 13, number 3, available at http://www.uic.edu/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/2142/1949.

[18] The colourful term is not my own. Hedley Bull came up with it in 1977, in his *The Anarchical Society. A study of order in world politics*, MacMillan, London.