Conjuntura Austral

RECENT DEVELOPMENTS OF CYBERSECURITY AND ITS IMPLICATIONS TO INTERNATIONAL RELATIONS: STRATFOR VERSUS ANONYMOUS.

Desdobramentos Recentes da Segurança Cibernética e as suas Implicações para as Relações Internacionais: Stratfor versus Anonymous.

Bernardo Wahl Gonçalves de Araújo Jorge[1]

In December 2011, the "hacker movement" *Anonymous* claimed the theft of private data, including credit card numbers, of approximately 860.000 clients of the consulting and intelligence analysis enterprise *Stratfor* - acronym for *Strategic Forecasting*. (DILANIAN, 2012). George Friedman, the owner of the company, stated that the attack aimed to "silence *Stratfor*" through the destruction of its data and website (FRIEDMAN, 2012). In the following paragraphs, a brief overview of the international relations in the last years will be outlined for a proper contextualization of the issue.

In 2002, Joseph S. Nye described the distribution of power among nations as a "complex three-dimensional chess game" (NYE, 2002: 80). The board above represented the military power, which was predominantly unipolar, i.e., concentrated in a single pole; in this case, the United States. The middle board represented the economic power, which was multipolar, i.e., distributed among several poles of power: the United States, Europe and Japan - with a great possibility of China arising as a main actor, which indeed happened. The bottom board represented the transnational relations

[1] Master in Peace, Defense and International Security Studies ("Prodefense" - initiative from the Department of Defense and from CAPES). Post-Graduation in International Relations Program from UNESP, UNICAMP and PUC-SP ("San Tiago Dantas" – initiative from CAPES). Invited professor of International Security at the course of Post-Graduation lato sensu Politics and International Relations at Fundação Escola de Sociologia e Política de São Paulo (FESPSP). Professor of International Relations at Faculdades Metropolitanas Unidas (FMU). E-mail: bernardowahl@gmail.com.

domain, which surpassed the national borders and escaped from the governmental control. The latter board included non-state actors of various kinds: from bankers to hackers and "terrorists".

More recently, the above-mentioned author updated his reflections on power in the book *The Future of Power* (2011). Among other ideas introduced, Nye identifies two changes in his object of study, alterations that are occurring in the 21th century: the power transition - in this case, to Asia - and the power diffusion - more specifically, the "cybernetic power", which diffuses to other actors than the nation-State. The first modification is an already known historical event (i.e., there were other transitions of power, from United Kingdom to the United States, for example), but the second transformation is a new process. The difficulty for all States in the current era of global information is that many events are happening beyond their control, including even the most powerful States (NYE, 2011:113).

Therefore, maybe now would be the appropriate occasion to update the "complex three-dimensional chess game" mentioned previously. It is relevant to introduce here the concept of cyberwar, defined as "a hostile action in the cyberspace, which effects amplify or are equivalent to an enormous physical violence" (NYE, 2012). The most intense modification occurs in the scope of the third level. In spite of the continuation of the existence of the military, economic and transnational spheres, the information revolution has been turning the scenario more complex. The cybernetic space is becoming more relevant, and this has implications for the international politics. Regarding cybernetic security, Misha Glenny thinks the cyberspace as a "seven-dimensional chess match", in which one can never be sure about who is the opponent (GLENNY, 2011:19). From the three-dimensional chess board to the seven-dimensional one, it is clear that the international relations became more complicated, a great deal due to the cyberspace.

This is the moment to resume the *Stratfor* and *Anonymous* case. What each one of these actors represent and what are the possible implications of the incident at issue for the contemporary international relations? With the end of Cold War and the beginning of the globalization phenomenon through the multiplication of the liberal

democracy, the intelligence capacity of the States, once turned to other states' threats, the traditional threats - in the conflict between capitalism and socialism - has begun to point toward economic intelligence. *Stratfor* must be seen under this context. It is possible to state that the company innovated by bringing to some internet users, through free informative publications, a type of knowledge once reserved to the State or to great organizations: the knowledge and the insights from intelligence analysis.

Anonymous, by its turn, can be seen as an idea, attached to a set of social and technical practices. It is diffuse and without a central leadership, a protest movement that inspires action inside and outside the internet, contesting the abuse of power by governments and corporations, aiming to promote transparency in politics and business. Often, however, *Anonymous* may go beyond the frontiers of legitimate protest, creating slightly distorted perceptions regarding the phenomenon. One of these distorted perceptions is the United States' one, more specifically embodied in the general Keith Alexander, in charge of the National Security Agency (NSA) and of the direction of the Cybernetic Command (the North-American military organ responsible for the operations in cyberspace), who began to realize *Anonymous* as a threat to the North American national security (BANKLER, 2012).

And, after all, what is in dispute? It is an updated version of the "great game" of international relations, now in the cyberspace, and not necessarily involving States directly. In these terms, the "great game" encompasses new actors - among them, *Stratfor* and *Anonymous* - which are not as big as States, but can cause some impact in international relations, in the cybernetic domain at least. *Stratfor* has a specific line of reasoning, a type of thinking that seeks to build opinions and to influence decisions. Nevertheless, the personal data of its clients were not encrypted, the minimum that is expected from a company that operates in the security area. *Anonymous*, astute as any hacker, took advantage from this error. Glenny states that there are three main threats in internet, and each one of them demonstrates in different ways. The first threat is the cybernetic crime; the second, the electronic industrial espionage and; the third, cyberwarfare (GLENNY, 2011: 234). Two "actors" are always present in all this

spectrum of threats: the spy (or, in a broader term, the intelligence agency, and here, the *Stratfor*) and the hacker (in the case described, the *Anonymous*).

Once more, it is appropriate to resume Nye in order to elucidate the question. In the real world, winning geography, projecting power by land, sea, air and cosmic space requires strategic projection capacity that only States own. In the virtual world, however, things are easier, i.e., it is much cheaper and faster to conduct bits and bytes through computers networks than it is to move aircraft carriers through oceans or bomber aircrafts through skies. The problem is: the obstacles to access the cybernetic space are very small. Thus, non-state groups and smaller States have the possibility to assume a relevant role, at an extremely low cost. Meanwhile, the most developed States, due to their dependence upon complex cybernetic systems for their military and economic actions (one should remember the "network-centric warfare"), are more vulnerable. The cyber space, in addition to being a pool of resources, becomes also an insecurity source for wealthy countries (NYE, 2012).

After the events of September 11, 2001, Thomas Barnett (2003) offered an explanation for the connection between globalization and the phenomenon of terrorism. According to Barnett, the attacks against the United States disclosed a new emergent geopolitical reality emerging at the time, the so called "new Pentagon map", in which the main international borderline were the one that separated the world of a "functional core" (consisting of developed and connected to the globalization countries, which believe in the "modernity") from a "non-integrative gap" (formed by countries that rejects the globalization, unconnected, mainly the called "failed States" or "bankrupt States"). Thus, at that moment, the threats would come from the "disconnected". Presently, as less developed States "connect" themselves, the cyber threats might increase, because the computers of the less developed countries are supposed to be more susceptible to viruses, malwares and to become slaves of botnets (robot networks) to, for example, distributed denial-of-service attacks (DDOS).

In sum, two phenomena, basically, can be observed. The first phenomenon is the power that non-state groups and small States can attain in the cybernetic space, and the relative insecurity of the develop countries, which infrastructures depends on the

cyberspace. The second phenomenon is the process of "connection" to the internet of the former non-connected countries, a process that, instead of bringing more safety (taking as starting point the Barnett rationale), paradoxically can introduce even more insecurity, at least in the perception of the most evolved States.

Finally, it is possible to connect one phenomenon to the other: the "connection" among the less developed countries could provide more cybernetic power capacity to small States and to non-State groups. In the real world, the States have almost the monopoly on the legitimate use of force. Nevertheless, this does not repeat necessarily in the virtual world. For this reason, it is important a closer examination concerning the incident between *Stratfor* and *Anonymous* and the process of connection to the internet of former non-connected States. All of them are small actors that can generate considerable impact on international relations.

REFERENCES

BARNETT, Thomas P. M. “The Pentagon’s New Map”. *Esquire*, March 1, 2003. Disponível em: <http://www.esquire.com/features/ESQ0303-MAR_WARPRIMER>. Acesso em 22 abr. 2012.

BENKLER, Yochai. “Hacks of Valor: Why Anonymous is not a Threat to National Security”. *Foreign Affairs*, April 4, 2012. Disponível em: <http://www.foreignaffairs.com/articles/137382/yochai-benkler/hacks-of-valor>. Acesso em 22 abr. 2012.

DILANIAN, Ken. “Hackers reveal personal data of 860,000 Stratfor subscribers”. *Los Angeles Times*, January 4, 2012. Disponível em: <http://articles.latimes.com/2012/jan/04/nation/la-na-cyber-theft-20120104>. Acesso em 22 abr. 2012.

FRIEDMAN, George. “The Hack on Stratfor”. *Stratfor Geopolitical Weekly*, January 11, 2012. Disponível em: <http://www.stratfor.com/weekly/hack-stratfor>. Acesso em 22 abr. 2012.

GLENNY, Misha. *Mercado Sombrio*: O Cibercrime e Você. São Paulo: Companhia das Letras, 2011.

NYE, Joseph. "Guerra e paz no ciberespaço". *O Estado de S. Paulo*, 15 abr. 2012, Internacional, p. A22. Disponível em: <http://www.estadao.com.br/noticias/impresso,guerra-e-paz--no-ciberespaco-,861242,0.htm>. Acesso em 22 abr. 2012.

_____. *The Future of Power*. New York: Public Affairs, 2011.

_____. *O Paradoxo do Poder Americano*. Por que a única superpotência do mundo não pode prosseguir isolada. São Paulo: Editora UNESP, 2002.

Translated by Eric Feddersen. Revised by Francine Ferraro.

Article received on April 22, 2012.Approved on June 15, 2012.

RESUMO

Este texto trata do incidente envolvendo a empresa *Stratfor* e o grupo hacker *Anonymous*, um episódio de segurança cibernética, tendo como objetivo refletir sobre as implicações do espaço cibernético para as relações internacionais.

PALAVRAS-CHAVE

Segurança cibernética, relações internacionais, poder.

ABSTRACT

This paper deals with the incident involving the company Stratfor and the hacker group Anonymous, an episode of cybersecurity, aiming to reflect on the implications of cyberspace for international relations.

KEYWORDS

Cybersecurity, international relations, power.