Stuxnet e defesa cibernética estadunidense à luz da análise de política externa

Stuxnet and the U.S. cyber defense under the foreign policy

Rev. Bra. Est. Def. ano 1, nº 1, jul./dez., p. 55-69

GILLS LOPES*
CAROLINA FERNANDA JOST DE OLIVEIRA**

1. INTRODUÇÃO

Este trabalho parte da hipótese principal de que os Estados Unidos da América (EUA) inovam sua política externa, a partir do momento em que a atrelam à arma cibernética conhecida por Stuxnet. Portanto, o objetivo aqui é realizar uma análise de política externa sobre a utilização do ambiente cibernético enquanto instrumental estadunidense, no século XXI, ponderando seus custos e benefícios. Ademais, busca-se também identificar de que maneira os EUA se utilizam do seu poder cibernético (*cyber power*) como alternativa para intervenção na questão iraniana.

Além desta seção introdutória e uma conclusiva, o presente artigo se divide em três partes principais: a primeira versa sobre os aspectos dos *small groups* dentro do governo estadunidense, que influenciam, de alguma forma, o processo de tomada de decisão de política externa; a segunda consiste em uma breve contextualização das implicações políticas sobre a questão nuclear iraniana e sua respectiva percepção por parte dos EUA, mais especificamente, do presidente estadunidense e de seu *staff*; e, finalmente, faz-se uma análise de política externa, a partir do exposto na segunda parte.

Como metodologia, elege-se o estilo qualitativo de análise, desenhando-se, como principal método, um estudo exploratório do caso Stuxnet-Irã. Nesse sentido, um objetivo específico se configura: apreender a postura do presidente dos EUA e de sua equipe, no que tange especificamente a essa questão.

Este trabalho parte do pressuposto de que, em um mundo cada vez mais

* Professor de Relações Internacionais da Faculdade Damas. Internacionalista (UEPB), Mestre e Doutorando em Ciência Política (Relações Internacionais) pela UFPE. Graduando em Redes de Computadores pelo IFPB. Bolsista do Pró-Estratégia (CAPES/SAE-PR).
** Graduanda em Relações Internacionais pela Universidade Federal da Paraíba (UFPB).

globalizado, em transformação (Villa e Reis 2006, 31), multipolar (Amorim 2001, 12), complicado (Flores 2004, 23) e interdependente (Kohler-Koch e Rittberger 2007, 3), dúvidas emergem acerca dos futuros centros de poder (Debates GACINT 2011, 1; Villa e Reis 2006, 32-33, 37) e sobre as principais ameaças estatais.

É nesse contexto de interdependência mundialmente complexa, e de dependência de sistemas informacionais, que a Sociedade da Informação do século XXI se depara com um ambiente de "(in)segurança cibernética", nos dizeres de Vaz (2012, 14).

Constata-se também uma crescente literatura acadêmica, que vincula políticas de combate a ameaças cibernéticas e políticas nacionais de defesa[1]. Em outras palavras, este século testemunha a securitização militar do ciberespaço (Lopes 2013) e, se depender do estudo de caso aqui analisado, tal premissa se fortalece ainda mais.

Um dos problemas de política externa com que Barack Obama teve de lidar, ao assumir a Casa Branca em 2009, foi quanto ao programa nuclear iraniano, o qual já envolvia altos oficiais das agências de inteligência, diplomáticas e militares (Clarke e Knake 2012, 292).

As aspirações iranianas de desenvolvimento de tecnologia nuclear remontam à Revolução Iraniana de 1979 (Hurst 2012, 545). Porém, em 2002, foi descoberto que aquele Estado construíra secretamente uma instalação de enriquecimento de urânio na cidade de Natanz.

Desde então, o Irã dominou as tentativas de "aproximação" estadunidense, que, além disso, objetivavam também à conquista de aliados no Oriente Médio (Hurst 2012, 546). Para Israel, em contrapartida, a postura que a Administração Obama tomou quanto ao caso se mostrou branda demais (Sanger 2012, 154-159).

Com os objetivos de neutralizar o programa nuclear iraniano e de não promover ataques militares convencionais para esse tento, o governo dos EUA lançou mão de um tipo de poder que atrela política externa a um novo ambiente de atuação das Forças Armadas: o poder cibernético.

Segundo Nye (2011, 123), poder cibernético é um conjunto de recursos que relaciona redes de informação, *software* e capacidades humanas e inclui, ainda, *intranets* e tecnologias celulares. Já Steed (2011, 22) divide esse conceito em cinco dimensões, sendo sua quarta a que interessa aqui: a otimização das Forças Armadas, por meio da produção de danos a uma rede de computadores inimiga, atacando os elementos cibernéticos que a sustentam.

Se as evidências que alguns autores[2] trazem a respeito da ferramenta cibernética desenvolvida para sabotar as instalações nucleares iranianas estiverem corretas, a utilização de armas cibernéticas, enquanto alternativa às incursões militares tradicionais, mostra-se como uma opção eficiente e financeiramente menos custosa de intervenção no programa nuclear iraniano, por parte dos EUA. É o que se pretende analisar a partir das seções seguintes.

2. A ANÁLISE DE POLÍTICA EXTERNA (APE)

De acordo com Hudson (2005, 1), Análise de Política Externa (APE) envolve principalmente tudo aquilo que ocorre entre os Estados e ao redor deles. Outrossim, considera-se que tal contexto é determinado pela ação de tomadores de decisão (*decision-makers*), agindo sozinhos ou em grupos. Assim, busca-se compreender como os seres humanos percebem e reagem ao mundo externo e, além disso, entender de que maneira eles moldam e são moldados por tal estado de coisas (*state of affairs*).

Nesse sentido, as variáveis da APE incluem o processo e os resultados da tomada de decisão humana, os quais têm múltiplas consequências e dimensões para entidades estrangeiras. Normalmente, os limites para a tomada de decisão se determinam por aqueles com autoridade para comprometer recursos. Em alguns casos, não se toma apenas uma única decisão, e sim uma sequência delas, com relação a uma mesma situação.

Tendo as tomadas de decisões como foco de análise, uma nova forma de se organizar os determinantes da ação emerge, em torno de tais indivíduos que agem no setor político. Pode-se caracterizar a tomada de decisão como um *comportamento organizacional*, em que variáveis – tais como esferas de competências e comunicação, bem como fluxo de informações – e motivações possuem papel imprescindível para a análise (Hudson 2005, 2-5).

Conforme o entendimento de Hudson (2007, 65), em momentos de crises, é importante que o líder seja capaz de se reunir com um conjunto de indivíduos, ou grupos (*small groups*), a fim de proceder com debates em relação às opções a serem tomadas.

Implementa-se a maioria das decisões de alto nível de política externa por meio de grandes organizações executivas, tais como Departamentos e Agências de Estado, as quais coletam e processam inicialmente as informações relevantes para uma dada questão pública. Nesse sentido, as organizações influenciam, de fato, na capacidade de o governo conduzir a política

externa, quando fornecem recursos que não são possíveis na sua ausência (Hudson 2007, 75).

Assim, as organizações têm a capacidade de ampliar os limites entre o tomador de decisão e as realizações políticas, i.e., elas podem ofertar a oportunidade de chegar-se mais além do que um líder poderia fazê-lo, agindo sozinho, na esfera política (Turner e Pratkanis 1998, 105).

Em contrapartida, ressalta-se que tais *small groups* também podem ser usados para explicar os fracassos de determinadas decisões políticas. Destacando o trabalho de Irving Janis, Hart (1991, 247) expõe que o fenômeno "pensamento de grupo" ("*groupthink*")[3] pode ser prejudicial dentro dos grupos elaboradores de política externa, ou seja, tais indivíduos possuem forte crença na capacidade de influência dos seus grupos, aliada a uma imagem não tão nítida dos adversários. Dessa forma, os resultados podem ser devastadores, gerando, por exemplo: visão distorcida da realidade; excesso de otimismo; e negligência ética. A combinação desses resultados tende a tornar tais organizações vulneráveis e portadoras de dificuldade de manter um dado projeto, levando-se a fiascos políticos.

Uma vez expostos tais aspectos e conceitos, no que diz respeito à participação dos *small groups* no processo de formulação de política externa, é possível analisar o caso Stuxnet-Irã, em que tais pressupostos podem ser identificados.

3. O STUXNET E O PROGRAMA NUCLEAR IRANIANO: COLOCANDO EM PRÁTICA UMA POLÍTICA EXTERNA E DE DEFESA CIBERNÉTICA

A localização geográfica do Irã lhe confere uma posição estratégica no Oriente Médio: encontra-se no centro da Eurásia. Além disso, é possuidor de grandes reservas petrolíferas e demonstra interesse em obter tecnologia nuclear, levantando suspeitas da comunidade internacional (Hurst 2012, 546; Lazier 2005, 1-2). Ressalta-se, ainda, o fato de o governo iraniano ser abertamente antiestadunidense e anti-israelense.

Desde o início do século XXI, o Irã está na mira das desconfianças dos EUA e da União Europeia, no que diz respeito a suas atividades com o manuseio de energia nuclear. Frente a isso, o governo iraniano argumenta que suas atividades nucleares têm, sim, fins pacíficos, alegando, ainda, a necessidade de haver um programa para a obtenção de fontes de energia mais eficientes e para o aumento do escopo de sua medicina. Dessa forma, o

Irã não considera suas atividades nucleares ilegais, nem aceita o fato de que elas estejam em desacordo com o Tratado de Não Proliferação de Armas Nucleares (TNP) (Gontijo 2005).

O fato de o Irã, como signatário do TNP, deixar de prestar informações sobre seu programa nuclear alimenta a desconfiança de que seus objetivos não se resumem à mera produção de energia nuclear para fins energéticos e medicinais, e sim de que ele está desenvolvendo armas nucleares. Em decorrência dessas suspeitas, são feitas investidas, por parte de EUA e Israel, a fim de descobrir mais detalhes sobre o programa e justificar, antecipadamente, uma intervenção nas instalações nucleares do Irã (Germer et al. 2009, 2; Sanger 2012, 143).

A administração W. Bush considerou como urgente a questão sobre o que fazer acerca desse imbróglio. Segundo Sanger (2012, 155), o *staff* do Presidente estadunidense lhe apresentou uma arriscada, mas tentadora proposta: inserir forças especiais no território iraniano, a fim de sabotar as instalações nucleares. Porém, os custos políticos e materiais dessa investida seriam altos demais em caso de fracasso. Outra opção, seria deixar o Irã construir as bombas, o que também não se mostraria viável para resolver o problema (Hurst 2012, 546).

Para W. Bush, tomador de decisão-mor dos EUA, uma terceira via seria vital, já que o problema do Irã não poderia esperar. Surgiu, então, a possibilidade da utilização do poder cibernético como alternativa de intervenção, dando origem a uma guerra cibernética, de frente única, contra o Irã (Sanger 2012, 154, 191-193).

É nesse ponto que Milevski (2011, 64) assevera que o poder cibernético se prostra como um desafio militar desde seu próprio surgimento enquanto conceito estratégico, o qual vem crescendo, principalmente, graças às revelações dos ataques cibernéticos às instalações nucleares iranianas. Nesse sentido, o poder cibernético está inexoravelmente atrelado ao conceito daquilo que a literatura sobre defesa cibernética chama de guerra cibernética (*cyber war*).

Conforme apontam Clarke e Knake (2012, 291), quando o termo guerra cibernética surge, é tido como algo meramente teórico. Em outras palavras, era difícil de se calcular, no início dos anos 1990, um ataque utilizando *software* que causasse danos a *hardware* de alguma infraestrutura crítica estatal. Essa opção surge, para o caso iraniano, de dentro do U.S. *Strategic Command* (USSTRATCOM), que há muito tempo se ocupava em aperfeiçoar o potencial bélico dos EUA. Porém, segundo Sanger (2012,

191), reconhece-se que, para os atuais conflitos de interesses estadunidenses, as antigas armas de persuasão estariam perdendo relevância, havendo a necessidade de se utilizar novos recursos. Dessa forma, tanto o *U.S. Department of Defense* (DoD) – a partir da criação do *U.S. Cyber Command* (USCYBERCOM) – quanto os órgãos de inteligência, de diplomacia e de segurança nacional se dedicam a desenvolver o potencial cibernético estadunidense como estratégia de segurança e defesa nacionais (Clarke e Knake 2012, 38-40).

Sendo uma proposta inédita, a intenção era de ,inicialmente, retardar os planos iranianos e ganhar tempo. Nesse sentido, desenvolveu-se um dos mais secretos programas dentro do governo dos EUA, o *Olympic Games* (Sanger 2012, 188-225), o qual possui dois objetivos políticos: sabotar, ainda que temporariamente, o programa nuclear iraniano e convencer Israel de que há uma maneira mais eficaz e menos custosa de lidar com o problema nuclear iraniano do que lançar ataques aéreos (Sanger 2012, *passim*). Em tese, o projeto se mostrou eficaz, mas, na prática, não havia garantias de que *de facto* funcionasse. Mesmo assim, Washington e Tel Aviv consideraram essa a melhor opção (Sanger 2012, 190-193).

Um *software* foi, então, concebido e aperfeiçoado pela Agência Nacional de Segurança de Israel e compartilhado com os EUA, tendo os israelenses uma participação fundamental na introdução do *malicious software (malware)* no sistema das centrífugas iranianas (Sanger 2012,195-196).

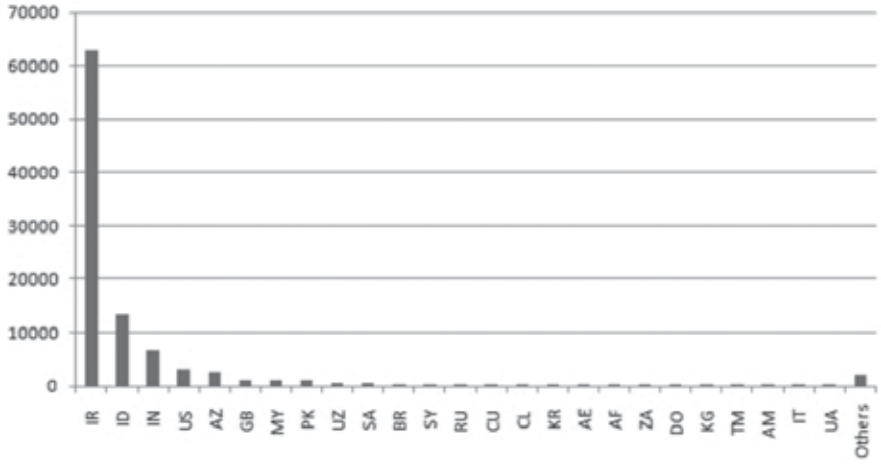
Nesse contexto, surgiu o que ficou conhecido depois por Stuxnet, um verme de computador (*worm*) utilizado como arma cibernética, cujos alvos são as centrífugas para enriquecimento de urânio, situadas em Natanz (Clarke e Knake 2012, 291-294; Foltz 2012, 44). O objetivo dos engenheiros especialistas em computação e física nuclear, dos EUA e de Israel, era explorar a vulnerabilidade das máquinas iranianas mapeadas pelos informantes israelenses. A intenção era fazer com que as centrífugas parassem de funcionar, de modo a parecer acidental, e que os engenheiros iranianos não desconfiassem imediatamente que estariam sob ataques cibernéticos. O Stuxnet seria introduzido no sistema computacional em Natanz, fazendo com que elas funcionassem de maneira inesperada, até quebrar. Com sorte, para EUA e Israel, parte dessas infraestruturas explodiriam e os iranianos demorariam a descobrir a origem do problema (Clarke e Knake 2012, 291, 295; Sanger 2012, 189).

Em 2010, o *worm* se comportou de maneira inesperada – espalhando-se para além de Natanz –, quando foi identificado e divulgado por especialistas em computação. A partir daí, o Stuxnet foi "capturado" por especialistas, os quais o perceberam como um sofisticado instrumento para proferir ataques

em rede a ser direcionado a outros alvos (Clarke e Knake 2012, 296).

O Gráfico 1 mostra a porcentagem de *hosts*[4] infectados pelo Stuxnet, em 2010.

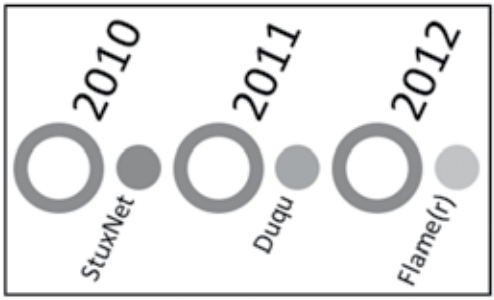
Gráfico 1 – Hosts infectados pelo Stuxnet, por país (2010)



Fonte: Falliere et al. 2011, 5.

Já o Esquema 1 apresenta as principais variante do Stuxnet, entre 2010 e 2012.

Esquema 1 – Linha do tempo do StuxNet e suas variantes



Fonte: Lopes 2013, 49.

Após a descoberta do erro que fez com que o Stuxnet se espalhasse pela Internet, realizaram-se reuniões dentro do DoD e da CIA para determinar os danos diplomáticos aos EUA: um deles foi o de poderem ser acusados de utilizar armas cibernéticas contra outro Estado, igualmente soberano, fazendo com que perdessem credibilidade no cenário internacional. Obama

recorreu a seus assessores[5], para avaliar os benefícios trazidos pelos ataques, que, de maneira geral, fizeram o Presidente estadunidense ganhar tempo (Clarke e Knake 2012, 296) e abrir oportunidades para reunir aliados e pressionar por sanções mais eficazes contra o Irã (Sanger 2012, 205).

Porém, tais ataques cibernéticos não foram suficientes para solucionar a questão por completo, de modo a fazer com que o Irã desistisse de seu projeto. Além disso, pelo fato de o Stuxnet ter escapado para as mãos de indivíduos em todo o mundo, os EUA também lançaram uma arma que um dia pode ser usada contra suas próprias infraestruturas críticas. Tem-se, portanto, uma ferramenta bem planejada tecnicamente, mas mal concebida estrategicamente.

Tendo em vista o objetivo de mesclar política externa com política de defesa cibernética, torna-se imperioso uma análise do caso precitado à luz da APE.

4. APE E O CASO STXUXNET

No que diz respeito à APE, nesse cenário, evidencia-se alguns aspectos apresentados por Hudson (2007) na política externa estadunidense. A autora explica como a interação dos grupos ou organizações dentro do governo pode favorecer o processo de tomada de decisão política. Vê-se, no caso em tela, que, como a autora defende, o processo decisório se dá através do líder político – neste caso, o presidente dos EUA – e de sua equipe. Além disso, a partir do momento em que se identifica uma "crise", o líder se reúne com um conjunto de indivíduos/*experts*, a fim de proceder com as discussões sobre as opções para a intervenção. Por ser uma questão de alto nível de política externa estadunidense, toma-se a decisão final com o apoio de grandes organizações executivas: Departamentos de Estado e de Segurança Nacional, DoD e CIA.

No caso Stuxnet-Irã, a atuação desses grupos ao desenvolver novas alternativas de intervenção, mais vantajosas para os EUA, se mostra visceral, sendo responsáveis tanto pelo processo de coleta de dados e processamento de informações, quanto pela oportunidade de se descobrir novas formas de poder para seu país. Para alcançar os objetivos traçados, a partir das informações coletadas, tais organizações trabalharam no sentido de possibilitar novas opções para o tomador de decisão, comprovando o que Hudson (2007, 75) sustenta: governantes percebem e agem, principalmente, por intermédio de organizações. Nesse contexto, o governo dos EUA

utiliza a burocracia nacional como um instrumento, a fim de chegar à solução mais eficazmente possível para o caso em tela.

A participação de Departamentos e Agência estadunidenses na questão iraniana proporciona a possibilidade de investir em alternativas de utilização de poder no ciberespaço. Sem a influência desses organismos, o limite de ação se restringe a duas opções: permitir que o Irã prossiga livremente com seu programa nuclear – buscando-se, assim, sanar o problema por intermédio de sanções do Conselho de Segurança da ONU ou da AIEA, por exemplo – ou intervir militarmente, utilizando-se de ataques aéreos israelenses contra o Estado iraniano. Nessas condições, os *small groups* permitiram ao tomador de decisão iniciar um programa secreto de intervenção na política de outro Estado soberano.

Como mencionado, o programa idealizado no governo W. Bush e continuado por Obama tem basicamente dois objetivos: retardar os planos iranianos e dissuadir Israel de atacar o Irã – uma vez que essa medida significaria mais uma guerra naquela região –, convencendo-o de que existiam opções melhores. A criação do Stuxnet, idealizado e utilizado como arma cibernética, só é possível graças à ação conjunta das organizações governamentais dos dois países envolvidos.

Quando o *worm* se espalha pela Internet, é igualmente importante a atuação dos grupos dentro do governo, para garantir ao líder político que os estragos não sejam tão graves e que, apesar do erro assumido, o programa alcance seus objetivos, uma vez que sabota algumas centrífugas e neutraliza a possibilidade de mais uma guerra no Oriente Médio.

Portanto, baseado em Hudson (2007), é possível perceber, a partir da APE, quanto ao caso em estudo, que existe uma participação fundamental dos *small groups* no processo de tomada de decisão do governo dos EUA. Isso se materializa, principalmente, por meio de coleta e tratamento das informações necessárias para se programar uma ação mais eficaz e menos político e economicamente custosa, principalmente para os EUA.

5. CONSIDERAÇÕES FINAIS

A utilização do ciberespaço e de armas cibernéticas como elementos de política externa, por parte dos EUA, e em relação à questão nuclear do Irã, constitui uma manobra inédita, já que, até pouco tempo atrás, qualquer menção sobre uma intervenção desse tipo era considerada improvável.

Esses novos instrumentos só são possibilitados em decorrência da ação

eficiente das organizações governamentais que, ao trabalharem seguindo as instruções dos seus líderes, ampliam os horizontes do processo de tomada de decisão para tal questão. Isso exemplifica o que Hudson (2007) explica sobre a importância da utilização dos *small groups* dentro do governo para determinar os meios da política externa. Mesmo com a tendência à concorrência entre esses grupos – que podem levar à vulnerabilidade e ao fracasso de decisões políticas –, existindo coordenação e envolvimento do líder no processo decisório, os organismos podem ser considerados benéficos.

Outro aspecto relevante é que, a partir do erro de comportamento do Stuxnet, a postura dos EUA quanto à utilização do ciberespaço fica publicamente exposta. Assim, eles transformam sua atuação cibernética em uma nova forma de projetar poder no sistema internacional (poder cibernético). Ao contrário, pode também engendrar uma nova vulnerabilidade: outros atores podem seguir seu exemplo, gerando um efeito reverso, i.e., transformando os próprios EUA, em um alvo em potencial de suas próprias armas cibernéticas, como visto com as variantes do Stuxnet. Tal preocupação já está incluída nas considerações iniciais de Obama (Sanger 2012).

Assim, é de se esperar que organizações que atuam nas áreas de defesa e segurança já estejam se preparando para esses novos tipos de ameaças, que, embora provenham do mundo virtual, podem causar danos cada vez mais reais.

NOTAS

1. Cf.: Brasil 2012; Canadá 2010; Estados Unidos 2011a, 2011b; Nye 2011.
2. Broad et al. 2011; Clarke e Knake 2012; Falliere et al. 2011; Hopkins 2011; Irã 2010, 2011; Milevski 2011; Sanger 2012; Steed 2011.
3. Forma excessiva de concorrência em busca de alto prestígio, pelos membros dos grupos, que tendem a valorizar a organização.4 Grosso modo, host é um equipamento – geralmente um computador ou roteador – conectado a uma rede de computadores, que, amiúde, serve de elo/nó de uma rede.
4. Grosso modo, host é um equipamento – geralmente um computador ou roteador – conectado a uma rede de computadores, que, amiúde, serve de elo/nó de uma rede.
5. O próprio Richard Clarke, autor da mais famosa obra sobre guerra cibernética, fora assessor de segurança internacional da Casa Branca.

RESUMO

O tema deste trabalho envolve um case de política externa estadunidense atrelada a uma política de defesa cibernética audaciosa, no que tange ao programa nuclear iraniano. Mais precisamente, analisam-se os impactos estratégicos trazidos pelo verme de computador Stuxnet, à luz da Análise de Política Externa.

Palavras-chave: Defesa cibernética. Análise de política externa. Stuxnet. Estados Unidos da América.

ABSTRACT

This paper has as its core a case study involving the U.S. foreign policy linked to its cyber defense policy, in regard to the Iranian nuclear program. More precisely, this work analyzes the strategic impacts brought by the Stuxnet computer worm, in light of the Foreign Policy Analysis.

Keywords: Cyber defense. Foreign policy analysis. Stuxnet. United States of America.

REFERÊNCIAS

Amorim, Celso. 2001. Reflexões sobre o mundo 'pós -11 de setembro'. *Panorama da Conjuntura Internacional* (12): 11-14, http://www.iri.usp.br/documentos/af43e8af44116918d717a77b936bd731.pdf. (Acessado em 12 abr. 2013)

Brasil. 2012. Política Cibernética de Defesa. *Diário Oficial [da] República Federativa do Brasil*. 27 dez. 2012(1): 11-12.

Broad, William J. et al. 2011. Israeli test on worm called crucial in Iran nuclear delay. *The New York Times*. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all. (Acessado em 5 mar. 2013)

Canadá, Sécurité publique. 2010. *Stratégie de cybersécurité du Canada*. http://www.publicsafety.gc.ca/prg/ns/cybr-scrty/_fl/ccss-scc-fra.pdf. (Acessado em 8 fev. 2013)

Clarke, Richard A., e Robert Knake. 2012. *Cyber war: the next threat to national security and what to do about it*. 2nd. ed. New York: HarperCollins.
Debates GACINT. 2011. *Informativo digital sobre os debates no âmbito do Grupo de Análise da Conjuntura Internacional* (1). http://www.iri.usp.br/documentos/DebatesGacint01.pdf (Acessado em 3 jan. 2013)

Estados Unidos. 2011a. *Strategy for Operating in Cyberspace*. http://defense.gov/news/d20110714cyber.pdf. (Acessado em 4 jan. 2013).

_____. 2011b. International *Strategy for Cyberspace*. http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (Acessado em 25 fev. 2013).

Falliere, Nicolas et al. 2011. *W32.Stuxnet Dossier*. Cupertino, CA: Symantec Corporation.

Flores, Mario C. 2004. Força, legitimidade e continuidade na mudança. *Panorama da Conjuntura Internacional* (22). http://www.iri.usp.br/documentos/1bf226c8df1e94cb94840b736feb0823.pdf. (Acessado em 10 abr. 2013).

Foltz, Andrew. 2012. Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate. *JFQ* 4 (67): 40-48.

Germer, André et al. 2009. O Irã Nuclear. *Centro de Estudos Estratégicos do Exército Brasileiro*. http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/47/71. (acessado em 20 mar. 2013).

Gontijo, Camila M. A. 2005. A questão nuclear no Irã. *Conjuntura Internacional* 2(11). http://www.pucminas.br/imagedb/conjuntura/CNO_ARQ_NOTIC20050705151127.pdf?PHPSESSID=d5971a7e9e2ede02ed3fb5dc071d1931. (Acessado em 20 mar. 2013).

Hart, Paul't. 1991. Janis' Victims of Groupthink. *Political Psychology* 12(2): 247-278.

Hopkins, Nick. 2011. Stuxnet attack forced Britain to rethink the cyber war. *The Guardian*. http://www.guardian.co.uk/politics/2011/may/30/stuxnet-attack-cyber-war-iran. (Acessado em 4 abr. 2013).

Hudson, Valerie M. 2005. Foreign Policy Analysis: actor-specific theory and the ground of International Relations. I*nternational Studies Association* 1. http://graduateinstitute.ch/webdav/site/political_science/users/jovana.carapic/public/Hudson_FPA%20Actor%20Specfic%20Theory%20and%20IR.pdf. (Acessado em 4 mar. 2013).

_____. 2007. *Foreign policy analysis: classic and contemporary theory.* New York: Rowman & Littlefield.

Hurst, Steven. 2012. Obama and Iran. *International Politics* 49(5): 545-567.

International Atomic Energy Agency. 1970. *Treaty on the non-proliferation of nuclear weapons.* http://www.iaea.org/Publications/Documents/Infcircs/Others/infcirc140.pdf (acesso em 29 mar. 2013).

Irã. 2011. Iran calls for IAEA to detect Stuxnet agentes. *Iranian Student's News Agency.* http://old.isna.ir/ISNA/NewsView.aspx?ID=News-1786952&Lang=E (Acessado em 3 abr. 2013).

_____. 2012. Identification of a new targeted cyber-attack. *Iranian Computer Security Incident Response Teams – CSIRT.* http://www.certcc.ir/index.php?name=news&file=article&sid=1894. (Acessado em 3 abr. 2013).

Kohler-Koch, Beate e Berthold Rittberger, Ed. 2007. *Debating the democratic legitimacy of the European Union.* Lanham: Rowman & Littlefield Publishers.

Lazier, Tiago C. 2005. Atentados no Irã e no Iraque. *Conjuntura Internacional 2(23).* http://www.pucminas.br/imagedb/conjuntura/CNO_ARQ_NOTIC20051117122700.pdf?PHPSESSID=ee7d9e27f570426fb80daa1c5ef413fb (Acessado em 20 jan. 2013).

Lopes, Gills. 2013. *Reflexos da digitalização da guerra na política internacional do século XXI: uma análise exploratória da securitização do ciberespaço nos Estados Unidos, Brasil e Canadá.* Dissertação de Mestrado. Recife: Programa de Pós-Graduação em Ciência Política da UFPE.

Milevski, Lukas. 2011. Stuxnet and strategy: a special operation in cyberspace? *JFQ* 4(63): 64-69.

Nye, Joseph S. 2011. *The future of power.* New York: PublicAffairs.

Sanger, David. 2012. *Confront and conceal: Obama's secret wars and surprising use of American power.* New York: Crown Publishes.

Steed, Danny. 2011. Cyber Power and Strategy – So What? *Infinity Journal* 2: 21-24.

Turner, Marlene A. e Anthony R. Pratkanis. 1998. Twenty-five years of Group-think theory and research: lessons from the evaluation of a theory. *Organizational behavior and human decision processes* 73(2): 105-115.

Vaz, Alcides Costa. 2012. Relações internacionais em tempos de crise política. *Conferência Nacional de Política Externa e Política Internacional* (6): 13:26.

Villa, Rafael Duarte e Rossana Reis. A segurança internacional no pós-Guerra Fria: um balanço da teoria tradicional e das novas agendas de pesquisa. R. *bras. de Informação Bibliográfica em Ciências Sociais* (BIB) 62: 19-51.

Recebido em: 29/04/2013. Aprovado em: 10/07/2013.