O PAPEL DA DISSUASÃO NO TOCANTE A OFENSAS CIBERNÉTICAS [1]

Analista de Sistemas Marcelo Antônio Osller Malagutti

O analista de sistemas Malagutti graduou-se bacharel em Ciência da Computação pela Universidade de Brasília (UnB) em 1988. Possui o grau acadêmico de pós-graduação ao realizar mestrado em administração de negócios (*Master of Business Administration - MBA*) em Estratégia Empresarial pela Fundação Getúlio Vargas (FGV) em 2009. É diplomado pela Escola Superior de Guerra (ESG) ao realizar o Curso de Altos Estudos em Política e Estratégia (CAEPE) em 2010. Atualmente é mestrando em Estudos de Guerra no *King's College London*, na Inglaterra. Nos últimos vinte e dois anos foi empresário de setor de software de automação bancária (marcelomalagutti@yahoo.com.br).

A teoria da dissuasão se tornou popular durante a guerra fria, associada ao temor de uma guerra nuclear. O fim da União das Repúblicas Socialistas Soviéticas (URSS) em 1991 marcou o fim da guerra fria. Com ele, o medo de uma guerra nuclear diminuiu significativamente. Apenas dois anos depois ARQUILLA e RONFELDT (1993) declaram que a guerra cibernética está chegando. O medo dessa nova ameaça ocupa mais espaço, a cada dia, no imaginário popular, na mídia, na elaboração de políticas públicas e na academia, com debates sobre o que seria e se haveria (CLARKE 2010; STONE 2013) ou não haveria (RID 2012) tal guerra.

Computadores tornam-se a cada dia mais utilizados na vida moderna. Antigas (ou clássicas) práticas, como espionagem, sabotagem, furto, fraude, estelionato, sequestro, ativismo político e guerra, ganharam novos contornos e novos nomes, em alguns casos apenas pela adição do prefixo ciber (ou cyber), como em ciberespionagem ou cibercrime, e em outros casos neologismos, como em *cybotage* [2] (algo como cibotagem, em língua portuguesa), *ransomware* [3] ou *hacktivism* [4].

Quaisquer que sejam os nomes, um fato inquestionável é que números exponencialmente maiores dessas práticas são revelados a cada ano. Fossem tais ofensas relacionadas apenas a aspectos de segurança já seria motivo suficiente para que nações com elas se preocupassem e delas se ocupassem. Mas a partir do momento em que elas envolvem aspectos de defesa tornam-se, indubitavelmente, um assunto de importância nacional e internacional.

Algumas questões cruciais emergem. Terá a dissuasão um papel relevante contra ameaças cibernéticas? Quais são essas ameaças? Quem são seus perpetradores? Existem medidas efetivas que nações possam tomar para dissuadir os perpetradores de realizá-las? Quais são essas medidas? E quais os recursos necessárias para implementá-las?

Neste artigo demonstraremos que sim, existe um papel (e um consideravelmente grande) para dissuasão cibernética. Ele foi dividido em cinco seções. A primeira provê uma categorização das ofensas e de seus perpetradores. A segunda apresenta diferentes níveis de dissuasão. A terceira discute alguns problemas relativos à dissuasão cibernética. A quarta seção apresenta recomendações genéricas de implementação. Conclui-se com algumas considerações finais.

OFENSAS CIBERNÉTICAS E SEUS PERPETRADORES

YANO (2012) dividiu os perpetradores em quatro diferentes grupos: cibercriminosos, *hacktivists*, terroristas e nações. Estes grupos foram aqui combinados com definições dadas por CILLUFO, CARDASH e SALMOIRAGHI (2012). Cibercriminosos

foram ainda subdivididos em dois diferentes grupos: organizado e individual. Cada grupo tem diferentes motivações, escopo de ações, alvos e recursos.

Cibercriminosos individuais são pessoas ou grupos não organizados que usam o ciberespaço para cometer crimes, em geral motivados por lucro, impulsos sexuais, vingança, convicções políticas ou religiosas, ou apenas por diversão ou desafio. Eles são em geral altamente emocionais. Exemplos podem variar de ex-empregados de bancos a ex-esposas (ou ex-maridos), pedófilos ou jovens querendo testar suas habilidades tecnológicas. Seus recursos são limitados. Suas capacidades são também limitadas, embora alguns excepcionalmente habilidosos possam ser encontrados nesse grupo.

Cibercriminosos organizados são grupos do crime organizado [5] que, motivados pelo lucro financeiro, usam o ciberespaço para cometer crimes ou contravenções. Exemplos podem ser traficantes de drogas que simplesmente usam a internet como meio para suas operações, ou criminosos que roubam informações bancárias ou de cartões de crédito armazenadas nos computadores de suas vítimas e as ultilizam ou vendem, passando por aqueles que usam *softwares* que cifram as informações do disco rígido do computador e pedem resgate para decifrá-las (*ransomware*). Seus recursos são também limitados, embora maiores que os do primeiro grupo. Também o são suas capacidades, com o desenvolvimento autônomo de ferramentas ou a aquisição das mesmas no mercado negro (ou "*dark* web").

Hacktivists são motivados por uma causa, em geral agindo em desobediência civil. Com frequência focam a confidencialidade, integridade e disponibilidade (CID) da informação. Atuam sobre informação relativa a seus alvos, em geral pessoas ou corporações consideradas contra a sua causa. Seus recursos são quase sempre muito limitados em termos de material e de capacidades de desenvolvimento. Mas são altamente motivados e expertos no uso de suas ferramentas limitadas. A ameaça de vazamento de informações confidenciais, a desfiguração de *sites* e ataques de negação de serviços (*Denial of Service - DoS*) contra *sites* institucionais ou páginas pessoais são algumas de suas ofensas características.

Terroristas são motivados pela atração de publicidade para sua causa, provocando terror e usando o medo resultante para expandir o dano a seus inimigos. Geralmente almejam a integridade física de pessoas ou propriedades materiais. Ciberterrorismo pode ainda ser definido como o uso intencional de computadores, redes e internet pública como um meio para causar (ou suportar) ações cinéticas que causem a destruição ou dano físico a seus objetivos políticos, religiosos ou ideológicos. Seus recursos são geralmente maiores que aqueles dos grupos anteriores. Suas capacidades são também maiores, mas ainda limitadas. Exemplos de suas ações podem ser angariar recursos (financiamento coletivo, por exemplo), lavagem de dinheiro e recrutamento de soldados para a causa.

Ciberterrorismo pode ainda ser definido como o uso intencional de computadores, redes e internet pública como um meio para causar (ou suportar) ações cinéticas que causem a destruição ou dano físico a seus objetivos políticos, religiosos ou ideológicos.

Nações-estados têm diversas motivações. O caso Snowden (GREENWALD 2014) revelou duas: espionagem política, com chamadas telefônicas da Presidente do Brasil e da Chanceler Alemã sendo interceptadas, e espionagem econômica da Petrobras, a petroleira brasileira que em 2008 tornou público

o descobrimento de vastas reservas de petróleo nas águas jurisdicionais brasileiras. Outra motivação pode ser a projeção de poder e a negação de uso no domínio cibernético [6]. Como visto no caso Stuxnet (ZETTER 2011; FALLIERE, O'MURCHU e CHIEN 2011; LANGNER 2011), o objetivo pode ter sido sabotagem, se não um ato de guerra, com a destruição física de ativos, objetivos políticos e efeitos letais sobre "interesses vitais" de uma nação e a imposição de vontade externa sobre essa nação [13]. Como KISSINGER (2014) escreveu, "ele foi bem sucedido em interromper e atrasar os esforços nucleares iranianos, em algumas avaliações com efeitos equivalentes aos de uma ataque militar limitado" [7]. Os recursos desse grupo são virtualmente ilimitados, bem como as capacidades.

DIFERENTES NÍVEIS DE DISSUASÃO

Em seu conceito clássico, dissuasão é a capacidade de desencorajar ou persuadir alguém no sentido de que não faça alguma coisa.

Historicamente, uma nação detentora de grandes capacidades militares dissuadiria seus rivais de atacá-la pelo medo de retaliação. Durante a guerra fria, a destruição mútua assegurada fez com que tanto os Estados Unidos da América (EUA) quanto a URSS tivessem medo de usar seus arsenais nucleares, garantindo a paz nuclear. Esse medo da retaliação destrutiva veio a ser conhecido como dissuasão nuclear e foi conceitualmente denominado dissuasão pelo medo ou pela ameaça de punição. A dissuasão é modelada como o produto de duas variáveis: capacidade e credibilidade. Isso foi objeto de estudos de BRODIE (1959), SCHELLING (1960 e 2014) e GANGHUA e YONGXIAN (2007). Em termos simples, a dissuasão pelo medo depende de se possuir os meios para retaliar e da sinalização da vontade ou disposição de se utilizar tais meios.

YOST (2003) e DAVIES (2014) discutiram diferentes níveis de dissuasão. Além da dissuasão pelo medo, existe também a dissuasão pela negação, que consiste em persuadir o inimigo a não atacar convencendo-o de que seu ataque será derrotado, ou seja, que ele não será capaz de atingir seus objetivos.

Yost observou o deslocamento feito pelo Departamento de Defesa dos EUA, particularmente depois do 2001 *Quadrennial Defense Review*, colocando *dissuasion* como complementar a *deterrence* na estratégia norte-americana. Como ele escreveu,

> os documentos oficiais de estratégia sugerem que *dissuasion* deve ser obtida pelo convencimento do adversário da futilidade de ele competir com os EUA, seja em bases gerais ou em uma categoria particular do poder militar.

Não se trata aqui mais de uma questão de temor da retaliação (dissuasão pelo medo), ou do temor de ser derrotado (dissuasão pela negação). O uso do termo futilidade está conectado ao conceito econômico da utilidade, onde investir em algo demanda um retorno do investimento. RUMSFELD (2002) exemplificou o conceito nos seguintes termos:

> A mera existência da U.S. Navy (Marinha dos EUA) dissuade outros de investirem em marinhas competitivas – pelo fato de que elas custariam uma fortuna e não lhes proveriam uma margem de vantagem militar – e desenvolveremos novos ativos, cuja mera posse dos mesmos desencoraja adversários de competirem.

Assim, a dissuasão pode ser obtida pelo convencimento do oponente quanto ao menos uma de três coisas: primeiro, da futilidade de se investir no desenvolvimento em armas de ataque (que denominaremos aqui dissuasão pela futilidade); segundo, de que seu ataque não superará as defesas (dissuasão pela negação); terceiro, de que seu ataque, quando bem sucedido, enfrentará um contra-ataque, não necessariamente proporcional (dissuasão pelo medo).

PROBLEMAS PARA IMPLEMENTAÇÃO DA DISSUASÃO CIBERNÉTICA

Dados os diferentes níveis (ou tipos) de dissuasão e categorizadas as ofensas e seus

perpetradores, quais são as dificuldades de se implementar a dissuasão cibernética?

Analisemos cada nível de dissuasão, em sua ordem cronológica.

Em termos de dissuasão pelo medo, uma grande dificuldade é determinar o que os ofensores temem. Cada grupo perpetrador, por sua natureza, tem um medo distinto. Cibercriminosos individuais, sendo emocionais, em geral não pensam a respeito da lei, embora usualmente a temam. Cibercriminosos organizados já estão costumeiramente confrontando agentes da lei no mundo físico. Se eles não temem prisões reais (ou mesmo tiros) o que temeriam no ciberespaço? Perder seu dinheiro parece ser seu único temor. Terroristas aparentam temer apenas a destruição de suas células ou grupos sem que tenham atingido sua missão. *Hacktivists* geralmente atuam no limite da legalidade e são apaixonadamente conectados a suas causas. Consequentemente eles não têm muito a temer, exceto, talvez, pela perda de seu anonimato. Uma vez expostos, eles se tornam monitoráveis e passíveis de responsabilização por seus atos. Nações, na ausência de uma legislação internacional específica, temeriam apenas retaliação, seja ela no ciberespaço ou naquele físico, por ações militares cinéticas ou sanções econômicas. Conforme escrito por KISSINGER "se um ciberataque é limitado a uma função ou extensão particular, uma retaliação do mesmo tipo pode ter implicações totalmente diferentes para os EUA e para o agressor". A dependência que a vítima inicial tem daquela função pode ser totalmente diferente daquela do agressor. Por exemplo, o Brasil tem um dos sistemas financeiros mais automatizados e mais dinâmicos do mundo. Se esse sistema sofresse um ataque de uma nação com menor nível de automação e dependência, uma retaliação a esse sistema não teria o mesmo efeito. Em qualquer caso, no entanto, é demandado o desenvolvimento dos meios, as capacidades necessárias e suficientes, e também a sinalização da disposição de emprego desses meios.

Outra importante dificuldade é relacionada ao problema da atribuição. É relativamente fácil a atribuição de uma ataque militar a um determinado país e então se iniciar um contra-ataque, e se possuindo suficiente poderio, ao fim e ao cabo superar e derrotar o oponente. Como NYE (2015) apontou, mesmo que a atribuição nuclear não seja perfeita, existem apenas uns poucos países com armas nucleares, os identificadores isotópicos de suas armas são relativamente bem conhecidos, e atores não-estatais enfrentam elevadas barreiras à entrada. Mas, como RID e BUCHANAN (2015) escreveram, a atribuição de ciberataques não é uma tarefa fácil. O uso costumeiro de falsas bandeiras [8] para encobrir a origem dos ataques poderia provocar uma retaliação contra uma nação inocente, o que poderia por em risco a credibilidade da capacidade de dissuasão e ter efeitos diplomáticos desastrosos no contexto internacional.

A dissuasão pode ser obtida pelo convencimento do oponente para que não invista no desenvolvimento de armas de ataque (futilidade), de que seu ataque não superará as defesas (negação) ou que enfrentará um contra-ataque desproporcional (medo)

A dissuasão pela negação fundamenta-se na capacidade técnica do defensor em implementar negação de uso de seu ciberespaço para a realização de atividades indesejáveis. O problema é que não existem defesas invulneráveis. Nem no mundo físico nem naquele

virtual. Uma típica ameaça persistente avançada, tradução do original em língua inglesa *advanced persistent threat* (APT) é uma ferramenta de ataque multiestágio baseada no modelo da *cyber kill chain* (HUTCHINS 2011). A premissa desse modelo é que a mitigação em qualquer estágio quebra a corrente e frustra o adversário. Assim qualquer repetição pelo adversário é passível de ser reconhecida pelos defensores que devem reconhecê-la e alavancarem sua reação. APTs são geralmente bem sucedidas pelo fato de que as defesas são usualmente baseadas em reconhecimento de padrões e apenas capazes de reconhecer eventos de alguns poucos estágios individualmente, mas não o ataque como um todo.

Em termos de dissuasão pela futilidade, persuadir cibercriminosos a não cometerem crimes no ciberespaço é provavelmente mais difícil do que no mundo físico. O mesmo se pode dizer a respeito de terroristas e *hacktivists*. Eles não desistirão, a menos que os custos se tornem injustificáveis. Nações, por sua parte, devem lidar com a clássica e sempre atual formulação de VEGETIUS [9]: *Si vis pacem para bellum* (Se desejas a paz, prepara-te para a guerra). Nenhuma nação pode decidir não investir em capacidades defensivas considerando que não vale a pena atacar. Capacidades defensivas importam. Nos termos de SCHELLING (2014):

> Pela força um país pode repelir e expulsar, penetrar e ocupar, apreender, exterminar, desarmar e incapacitar, limitar, negar o acesso, e diretamente frustrar uma invasão ou ataque. Pode, isto é, se ele tem força suficiente. Suficiente depende de quanto o adversário tem.

NYE (2015) observou o caso do ataque à Sony em 2014, o qual oficiais do governo dos EUA rapidamente atribuíram à Coreia do Norte, despertando ceticismo generalizado, até que algumas semanas depois um vazamento pela imprensa revelou que os EUA tinham acesso às redes da Coreia do Norte. Deveria a Coreia do Norte ser dissuadida pela futilidade de desenvolver dissuasão cibernética após esta revelação? E quanto ao Brasil após Snowden ter revelado que a Agência Nacional de Segurança dos EUA realizou ações de espionagem política e econômica em seus domínios?

O Exército Brasileiro, responsável pela segurança cibernética nacional, ao invés de adquirir um software antivírus estrangeiro, decidiu adotar um antivírus brasileiro, o qual já em 2014 passou a integrar o seleto grupo de melhores produtos do mercado.

POSSIBILIDADES DE IMPLEMENTAÇÃO DE DISSUASÃO CIBERNÉTICA

Dado o cenário acima, seria o caso de se desistir da dissuasão cibernética? A resposta é não! Desistir não resolveria nenhum dos problemas nem eliminaria nenhuma das ameaças. O cibercrime continuaria a crescer. Terrorismo, espionagem e sabotagem, patrocinados ou não por nações, tornar-se-iam práticas diárias. Assim, a questão é como obter os melhores resultados possíveis da dissuasão cibernética.

Em termos práticos a dissuasão é um sistema bastante dinâmico. Dessa forma, a abordagem de consciência situacional proposta por ENDSLEY (1995), abrangendo o uso de indicadores para o entendimento das capacidades e das ameaças reais deve ser a origem de qualquer política. Ela está, de fato, presente no uso de indicadores (atômicos, computados ou comportamentais) sugeridos por HUTCHINS em sua proposta de defesa de redes de computadores orientada por inteligência.

Entendida a situação específica, a implementação da dissuasão pode ser hierarquicamente organizada em políticas, estratégias, livros verdes e brancos, normas, manuais, guias, e, na última ponta, diretivas e atividades.

Ainda que os contextos sejam diferentes para cada país, recomendações genéricas de amplo espectro são possíveis, e foram aqui agrupadas por área.

1) Arcabouço legal

Equalizar o tratamento dos cibercrimes ao de seus equivalentes no mundo físico é um bom começo. Evita que os criminosos deixem de ser punidos pela falta da tipificação ou por conta de lacunas na legislação. Em seguida, a implementação de legislação específica para cibercrime. No caso brasileiro, a chamada Lei Carolina Dieckmann [10] foi um bom começo, ainda que um tanto tardio. Outra medida consiste na adequação da legislação para permitir a coleta de evidências e de informações de inteligência e seu uso para impor punição aos crimes cometidos no (ou suportados pelo) ciberespaço.

2) Educação e qualificação

Muitas das ciberofensas se aproveitam da inexperiência dos usuários em questões de segurança. Educar os usuários quanto às melhores práticas relativas à tríade CID já mencionada (confidencialidade, integridade e disponibilidade) de suas informações pessoais certamente elevaria os custos de muitas atividades criminosas, exercendo algum nível de dissuasão pela futilidade. A qualificação e treinamento de ciberinvestigadores forenses não seria diretamente um agente de prevenção ao crime, mas tornaria mais fácil enredar os cibercriminosos. Qualificar desenvolvedores de software na implementação de mecanismos de segurança e de resiliência de sistemas também é essencial, assim como o é o treinamento e certificação de analistas de segurança e o treinamento de equipes de resposta a incidentes cibernéticos, *cyber security incident response teams (*CSIRT).

3) Desenvolvimento de ferramentas e técnicas de investigação e atribuição

O desenvolvimento de ferramentas e técnicas que viabilizem a atribuição e a investigação (incluindo infiltração e espionagem), visando à obtenção de dados de inteligência e evidências criminais é também uma ação recomendada. É razoável pressupor que uma nação disponha de melhores capacidades e recursos que a maioria dos criminosos, terroristas ou *hacktivists.* No tocante a outras nações, uma das características mais relevantes do ciberespaço é sua assimetria. No exemplo de Rumsfeld para dissuasão pela futilidade, marinhas são muito caras para se competir contra potências mais desenvolvidas. Mas no domínio cibernético potências menores podem certamente alavancar seu poder a custos menores. Isso é especialmente verdadeiro se elas não pretendem atuar ofensivamente ou impor medo, mas apenas implementar dissuasão pela negação.

4) Arquiteturas de segurança

Sistemas críticos devem ser estanques ou isolados por *air gaps* [11] sempre que possível e, quando não for possível, contar com sistemas de detecção de intrusão continuamente atualizados.

A elaboração de diretivas para sistemas de segurança padrão em conformidade com o modelo do *cyber kill chain*, incluindo padrões de configuração das ferramentas, pode ser um ativo de enorme valor em termos de ganhos de tempo e efetividade, com rápida replicação de boas práticas. Essa medida também facilita a operação dos ciberinvestigadores forenses e dos *CSIRTs*, portanto reduzindo o tempo de reação e aumentando a resiliência, o que reduz os ganhos do atacante e portanto eleva o poder de dissuasão pela negação.

O uso da técnica de *red teaming* [12] para aferir o grau de segurança de sistemas também traz duplo benefício, assegurando tanto

neva Centre for Security Policy (GCSP) at http://www.gcsp.ch/Events/Cyber-9-12-Student-Challenge2.

Equipe constituída por mestrandos da França, Brasil, EUA e Cingapura finalista de um concurso realizado em Genebra, Suíça, promovido pelo *Geneva Centre for Security Policy (GCSP)*, *Atlantic Council* e *OTAN* para propor políticas de resposta a um cenário de evolução de um ataque cibernético.

a confiabilidade e resiliência dos sistemas quanto a própria proficiência dos próprios *red teams* e dos *CSIRTs*.

5) Adoção de melhores práticas internacionais

O ciberespaço oferece, nele mesmo, muitas boas fontes de informação gratuita sobre boas práticas. Governos publicam suas políticas, estratégias, diretivas, guias e relatórios em seus sítios oficiais. A Agência da União Europeia para Segurança de Redes e Informações, *European Union Agency for Network and Information Security (ENISA)* publica guias e recomendações em muitas línguas. O Centro de Excelência em Defesa Cibernética Cooperativa da OTAN, *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)* também provê boas recomendações práticas.

Em seu lado escuro a internet também provê muita informação e ferramentas de infiltração. Algumas são gratuitas, mas algumas ferramentas baseadas em falhas *zero-day* [13] podem custar centenas de milhares de dólares.

6) Desenvolvimento de tecnologia autônoma

É um fato: as portas dos fundos, *backdoors*, realmente existem em produtos comerciais. O relatório do Congresso dos EUA, *The US House Permanent Select Committee on Intelligence* (2012) fez diversas recomendações restringindo a aquisição de equipamentos de comunicação das gigantes chinesas Huawey e ZTE. Em dezembro de 2015 a empresa americana Juniper Networks anunciou

a descoberta de uma porta dos fundos secreta no sistema operacional de seus *firewalls* [14] (ZETTER 2015). É lógico presumir que tais portas dos fundos sejam, como de fato são, utilizadas por seus conhecedores para infiltrar sistemas que se baseiem nesses ativos.

Qualquer nação que pretenda elevar seu nível de segurança e dissuasão no ciberespaço não pode basear-se apenas em ativos de rede importados, pelo menos em seus sistemas críticos. MALAGUTTI (2010) sugeriu que o Exército Brasileiro (EB), responsável pela segurança cibernética nacional, ao invés de adquirir um *software* antivírus de uma companhia estrangeira deveria adquiri-lo de uma companhia brasileira, desenvolvendo tecnologia nacional nessa área e assegurando que infecções ou invasões não tirariam proveito de *backdoors* não documentadas. O EB de fato adotou o antivírus brasileiro *AVWare*, o qual já em 2014 passou a integrar o seleto grupo de melhores produtos do mercado internacional.

CONCLUSÃO

Como mencionado anteriormente, dissuasão é uma função de duas variáveis: capacidade e credibilidade.

Todas as recomendações acima relacionam-se às capacidades. Boas capacidades podem exercer influência dissuasiva. Uma vez que a dissuasão pela futilidade é relacionada a custos, elevando-se a qualidade da dissuasão pela negação elevaria os custos das ofensas, assim tornando-as proibitivas para diversos perpetradores. A mesma lógica pode ser aplicada no caso da dissuasão pelo medo. À medida que as apostas se tornam mais altas, alguns jogadores desistem do jogo.

Credibilidade, então, é o último ponto importante a ser observado. Ela não deve ser deixada para vir com o tempo, como um resultado de longo prazo das capacidades. Sinalização é essencial. O mercado ou público alvo precisa saber que as intenções são reais.

Criminosos e terroristas enfrentando a justiça normalmente constituem bons exemplos para mostrar que, no fim, o crime não compensa. Por outro lado, crimes que permanecem sem punição sinalizam a mensagem oposta. Nações com limitadas opções de contra-ataques ofensivos, seja por restrições de ordem legal ou pela falta de capacidades, podem fazer uso de boas capacidades de atribuição para claramente denunciar os ataques. Como visto no caso Snowden, uma vez que a atribuição é feita, a retaliação pode ser inteiramente diplomática ou mediática, promovendo embaraços diplomáticos e constrangimento político para os atacantes. A sinalização, nesse caso, foi positiva, de disposição para a retaliação. Embora no caso em tela a atribuição não tenha sido feita em decorrência das capacidades da vítima.

Boa sinalização é emitida quando um governo anuncia maciços investimentos em segurança cibernética ou que pretende contratar, ao longo dos próximos anos, centenas de técnicos para nela trabalharem [15]. Ou quando um ataque em larga escala, frustrado pelas defesas, é anunciado na imprensa, preferencialmente com a atribuição dos responsáveis. Sinalização pobre e mesmo provocativa ou desafiadora é emitida quando agentes públicos declaram a dificuldade de alocar valores relativamente pequenos em seus orçamentos para a implementação de defesas.

Críticos da teoria da dissuasão dizem que o fato de não ter ocorrido uma guerra nuclear não significa que foi devido à dissuasão nuclear. Em oposição, eu costumo argumentar que no domínio cibernético pode-se dizer que o fato de não se ter descoberto um ataque não significa que não se foi atacado.

Boas capacidade aliadas a boa credibilidade podem, no final das contas, prover razoável grau de dissuasão cibernética. E qualquer nível é melhor que nenhum!

REFERÊNCIAS

ADAMS, James. 2001. **Virtual Defense**, Foreign Affairs Volume 80 Number 3.

ARQUILLA, John e RONFELDT David. **Cyberwar is Coming!**, Comparative Strategy, vol. 12, 2, 1993, p.141-65

BRODIE, Bernard. 1959. **The Anatomy of Deterrence**, World Politics, Vol. 11, No. 2.

CILLUFO, Frank, e SHARON Cardash e SALMOIRAGHI George. 2012. **A Blueprint for Cyber Deterrence**: Building Stability through Strength, Military and Strategic Affairs, Volume 4, No. 3, December 2012

CLARKE, Richard, e KNAKE Robert. 2010. Cyber War, New York: Ecco.

DAVIES, Paul K. 2014. **Toward Theory for Dissuasion (or Deterrence) by Denial**: Using Simple Cognitive Models of the Adversary to Inform Strategy – Working Paper. RAND NSRD.

DAVIES, Paul K. 2014a. **Deterrence, Influence, Cyber Attack, and Cyberwar** – Working Paper. RAND NSRD

FALLIERE, Nicolas, O'MURCHU Liam and CHIEN Eric . 2011. **W32.Stuxnet Dossier**. Cupertino: Symantec Corporation.

GANGHUA, Xiang, and YONGXIAN Wang. 2007. **Preferences, Information and the Deterrence Game**, Chinese Journal of International Politics, Vol. 1, 309-345.

GREENWALD, Glen. 2014. **No Place to Hide**. London: Hamish Hamilton.

HUTCHINS, Eric, et al. 2011. **Intelligence-Driven Computer Network Defense Informed** by Analysis of Adversary Campaigns and Intrusion Kill Chains (paper presented at the 6th International Conference on Information Warfare and Security, George Washington University, Washington, DC, 17–18 March 2011).

KISSINGER, Henry. 2014. **World Order**. New York: Penguin Press.

LANGNER, Ralph. 2011. **Cracking Stuxnet**, a 21st century cyber weapon in TED Talks, https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_
cyberweap on, accessed on 07/03/2015.

MALAGUTTI, Marcelo. 2010. **Estratégia Nacional de Fomento à Indústria de Software**. Rio de Janeiro: ESG - Escola Superior de Guerra.

NYE, Joseph. 2015. **Can Cyber Warfare Be Deterred?**, Project Syndicate, available at http://www.project-syndicate.org/print/cyber-warfare-deterrence-by-joseph-s--nye-2015-12, accessed on 09/01/2016 at 18h45.

RUMSFELD, Donald. 2002.**Transforming the Military**, Foreign Affairs Volume 81 Issue 3.

RID, Thomas. 2012**. Cyber War Will Not Take Place,** Journal of Strategic Studies, vol. 35, 1.

RID, Thomas e Buchanan, Ben. 2015. **Attributing Cyber Attacks**, Journal of Strategic Studies, vol. 38:1-2, 4-37.

SCHELLING, Thomas. 1960. **The Strategy of Conflict**, London : Harvard University Press.

SCHELLING, Thomas. 2014. **Arms and Influence**, in Strategic Studies - A Reader, ed. By Thomas Mahnken and Joseph Maiolo, Oxon: Rutledge.

STONE, John. 2013. Cyber **War Will Take Place**, Journal of Strategic Studies, Vol. 36, 1, 101-108.

US House Permanent Select Committee on Intelligence. 2012. I**nvestigative Report on the U.S. National Security Issues** Posed by Chinese Telecommunications Companies Huawey and ZTE. Washington: US House of Representatives.

YANO, Edgar. 2012. **Defesa Cibernética**: Estado corrente e a evolução necessária para tratar as futuras ameaças do Ciberespaço, presentation in Cyber Warfare and Security Forum, Brasilia, Brazil, November 30.

YOST, David. 2003. **NATO Review Winter 2003**, available at http://www.nato.int/docu/review/2003/issue4/english/art4.html, accessed 24/11/2015 at 19h23.

ZETTER, Kim. 2011. **How Digital Detectives Deciphered Stuxnet**, the Most Menacing Malware in History, Wired Magazine, 11/07/2011.

ZETTER, Kim. 2015. **Secret Code Found in Juniper's Firewalls shows Risk of Government Backdoors**", Wired Magazine, 18/12/2015.

NOTAS

[1] É difícil uma tradução precisa para cyber-offences, de sorte que usarei uma tradução imperfeita, mas direta e bastante abrangente para contemplar o amplo conjunto de ameaças e transgressões do ciberespaço.

[2] Uma contração em língua inglesa de cyber-sabotage.

[3] Uma contração de ransom (sequestro) e software para indicar software para sequestro digital de informações.

[4] Uma contração de hacker (aquele que invade computadores) com activism (ativismo), denotando ativistas por computador.
[5] O Federal Bureau of Investigations (FBI), em seu glossário de termos, define crime organizado como qualquer grupo que possua uma estrutura formal e cujo objetivo primário seja a obtenção de lucro por meio de atividades ilegais.
[6] Desde 2010 os EUA consideram o ciberespaço o quinto domínio de guerra, ao lado da terra, mar, ar e espaço.
[7] Portanto atendendo a todos os requisitos Clausewitzianos para ser considerado um ato de guerra.
[8] Em língua inglesa false flags. Consiste na prática de se disfarçar a origem do ataque fazendo-o parecer originário de outra nação.
[9] Publius Flavius Vegetius Renatus, De Re Militari, Book III.
[10] Lei 12.737/2012, que recebeu o nome da atriz que teve fotos íntimas suas supostamente furtadas de seu computador em 2011 e divulgadas sem sua autorização.
[11] Denominação de se dá a sistemas que não se conectam a outros por meio de comunicação on-line, seja com ou sem fio.
[12] Classicamente os militares realizam simulações envolvendo um Time Azul e seu antagonista, o Time Vermelho. A técnica de Red Teaming consiste na utilização de um Time Vermelho para atacar o sistema alvo (defendido pelo Time Azul) sem que este último saiba precisamente como está sendo atacado.
[13] São falhas estruturais de sistemas, ainda não corrigidas por não terem sido identificadas pelos autores do sistema. No caso StuxNet acredita-se que o mesmo explorasse nada menos que três falhas zero-day (ou 0-day).
[14] Equipamentos para evitar o acesso não autorizado a redes de computadores.
[15] Como fez o governo britânico recentemente, anunciando o investimento de 1,9 bilhão de libras esterlinas (https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on- cyber-security).