FEMA, David Valdez

Falha na Defesa Cibernética: As Consequências Ambientais de Ações Hostis

Jan Kallberg e Rosemary A. Burk

UMA FALHA NA defesa cibernética pode ter efeitos mais amplos que os discutidos em debates anteriores sobre as possíveis consequências de um ataque cibernético. A necessidade de que a defesa cibernética proteja o meio ambiente não tem atraído a atenção que merece como uma questão de segurança nacional. Países adversários vêm, secretamente, buscando métodos para abalar e causar danos aos Estados Unidos da América (EUA) em um futuro conflito cibernético. O Presidente dos EUA observou essa questão no documento *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* ("Mantendo a Liderança Mundial dos EUA: Prioridades para a Defesa no Século XXI", em tradução livre):

Jan Kallberg é professor assistente na Arkansas Tech University e pesquisador assistente no Instituto de Pesquisa e Ensino sobre Segurança Cibernética da University of Texas – Dallas. É Ph.D. pela University of Texas – Dallas. Tem artigos publicados nas revistas Joint Force Quarterly, Strategic Studies Quarterly, Air and Space Power Journal, IEEE Access *e* IEEE Security and Privacy.

Rosemary Burk é professora assistente de Biologia na Arkansas Tech University. É Ph.D. pelo Departamento de Ciências Biológicas da University of North Texas. Suas pesquisas foram publicadas nas revistas International Journal of Water Resource Development *e* Journal of Freshwater Ecology.

> Tanto os atores estatais quanto os não estatais possuem a capacidade e a intenção de conduzir a espionagem cibernética e, potencialmente, ataques cibernéticos contra os EUA, com a possibilidade de graves efeitos sobre as operações militares e o território norte-americano[1].

O ex-Secretário de Defesa, Leon Panetta, apresentou uma avaliação clara sobre o risco desses ataques em um discurso proferido em 12 Out 12:

> Esses ataques marcam um agravamento significativo da ameaça cibernética, renovando preocupações de que cenários ainda mais destrutivos possam ocorrer. Sabemos, por exemplo, que atores cibernéticos estrangeiros vêm sondando redes de infraestrutura crítica dos EUA. Eles têm visado os sistemas de controle computacionais que operam estações químicas, elétricas e de tratamento de água, assim como os sistemas que regulam o transporte em todo o país.
>
> Sabemos de casos específicos em que intrusos obtiveram acesso a esses sistemas de controle. Também sabemos que eles vêm tentando criar ferramentas avançadas para atacar esses sistemas e provocar pânico, destruição e até mesmo a perda de vidas humanas[2].

Ainda que a liderança nacional tenha identificado o risco, manifestado preocupação e começado a alocar recursos para melhorar a defesa cibernética do país, outros consideram como sendo mínima a probabilidade de uma guerra cibernética. Um dos principais argumentos contra a possibilidade de uma futura guerra cibernética consiste na premissa de que um ataque desses não provocaria danos de longo prazo[3]. Esse argumento baseia-se em uma marginalização dos ataques cibernéticos como sendo interrupções intermitentes de computadores clientes por meio de programas rudimentares de *software* malicioso, que geram caos temporariamente[4]. A impressão é que os danos se restringem às redes de computadores atacadas, e não ao ambiente externo, que delas depende. Entretanto, as preocupações expressas pelo ex-Secretário de Defesa Leon Panetta, baseadas na observação feita pelo Presidente Obama, transmitem uma percepção mais ampla e holística quanto a potenciais danos além das redes de computadores.

Neste artigo, apresentamos um argumento claro de que a guerra cibernética pode infligir danos contínuos à sociedade visada, além da destruição de uma rede de computadores específica. As consequências ambientais de longo prazo de uma derrota em uma guerra cibernética e de uma falha na defesa cibernética nacional não têm sido devidamente consideradas. Os estudos intensos sobre segurança cibernética conduzidos na última década, com seu foco nas redes e em sua segurança, não trataram do risco para ambientes físicos que dependam de redes controladas ciberneticamente[5].

O Conceito de Guerra Cibernética

Em uma guerra cibernética, atores estatais buscam obrigar a parte adversária a mudar sua política. Portanto, a guerra cibernética deve ser considerada, primeiro, de um ponto de vista estratégico e, segundo, a partir de níveis inferiores de abstração. Um elemento central em todos os conflitos é o medo das consequências: as verdadeiras repercussões de uma oposição à determinação da parte que busca subjugar. As armas nucleares são temidas por terem efeitos confirmados e visivelmente devastadores. Será preciso demonstrar que as armas cibernéticas podem ser catastróficas; caso contrário, sua capacidade de ameaça ou dissuasão desaparece.

Estudos anteriores sobre a guerra cibernética tiveram como foco as interrupções na capacidade técnica ou militar e a resiliência, ou capacidade de recuperação, para operar em um ambiente degradado. O potencial para destruir os sistemas do adversário por meio da letalidade digital foi introduzido recentemente[6]. Nesses cenários, danos efetivos no longo prazo são limitados. Para um adversário que pretenda afetar a política norte-americana, as atuais vulnerabilidades em nossos sistemas de controle industriais são uma atraente oportunidade. Seus alvos podem levar a consideráveis impactos

sociais: medo, incerteza e pressão pública sobre a liderança política no caso de danos ambientais.

Atacar sistemas de controle industriais com o intuito de causar danos ao meio ambiente constitui um grave ato de guerra. Entretanto, enquanto não se puder identificar responsáveis e não houver um mecanismo de punição, fica a critério do agressor reconhecer proibições contra tais atos no direito internacional. Atualmente, existem poucas opções (se houver) para fazer com que um ator responda por ataques cibernéticos com base no direito internacional.

Efeitos Ambientais de uma Guerra Cibernética

Um oponente que tivesse a capacidade de causar danos consideráveis e irreversíveis aos EUA por meio de ataques cibernéticos contra sistemas de controle industriais, ou mesmo de obter controle, somente, sobre vários sistemas, limitaria as opções de política dos EUA. A ameaça e risco de um ataque cibernético teriam de ser considerados, e isso concederia a uma potência menor um efeito multiplicador de forças em um conflito direto com os EUA.

A quantidade de ataques cibernéticos conduzidos contra a infraestrutura do país na última década é motivo de grande preocupação para o governo federal[7]. Esses ataques foram ampliados, de modo a incluir sistemas de Controle de Supervisão e Aquisição de Dados (*supervisory control and data acquisition — SCADA*), que fazem parte dos sistemas de controle industriais. Os sistemas SCADA controlam os processos nos setores energético, de transporte e de gestão de recursos hídricos, entre outros. São a espinha dorsal na estrutura técnica de nossa sociedade. Tais sistemas podem permanecer viáveis durante décadas dependendo dos processos e máquinas que eles controlam. Entretanto, não têm, muitas vezes, a capacidade necessária, ou não são passíveis de uma fácil atualização para atender aos desafios de segurança cibernética contemporâneos. Muitos desses sistemas não foram projetados para serem conectados a um outro computador, muitos menos ligados a uma rede mundial de informações como a internet. A gama de vulnerabilidades aumentou drasticamente, à medida que sistemas embutidos de *software* passaram a ser uma característica comum em máquinas eletromecânicas. Esses controladores programáveis em companhias industriais e de serviços públicos têm poucos recursos de segurança cibernética. O fortalecimento e aumento da segurança dos sistemas SCADA norte-americanos devem levar décadas. Esses sistemas, em sua maioria, não passam por uma atualização depois de instalados, necessitando de *hardware* adicional para sua proteção. A defesa desses sistemas é a defesa em profundidade, envolvendo empresas e municípios, assim como o Departamento de Defesa e outras agências federais. Os componentes mais capazes nessas camadas de defesa integram o âmbito federal. A questão é a seguinte: o que pode acontecer caso a segurança cibernética falhe? As ramificações ambientais merecem o mesmo grau de atenção que a possível ameaça aos sistemas computacionais.

Barragens e Represas Hidrelétricas

Uma série de falhas nas barragens de uma grande bacia hidrográfica teria, por exemplo, consideráveis impactos ambientais. As barragens e represas hidrelétricas são controladas por meio de diferentes tipos de redes de computadores, com ou sem fio, e essas redes de controle estão conectadas à internet. Uma falha na defesa cibernética de uma companhia elétrica poderia chegar aos controladores lógicos que fazem o maquinário elétrico abrir as comportas. Muitas barragens e represas hidrelétricas são projetadas em cadeia em grandes bacias hidrográficas, a fim de produzir um fluxo determinado de água para gerar energia. Um ataque cibernético contra algumas barragens a montante poderia liberar um volume de água que aumentasse a pressão nas barragens a jusante. Com a rápida diminuição da capacidade de armazenagem, as barragens a jusante correriam o risco de romper com o fluxo de água. Isso poderia acabar tendo um efeito cascata, literal e figurativamente, por todo o sistema fluvial, resultando em uma inundação catastrófica. O modo tradicional de enquadrar o problema em termos de segurança cibernética

Adam DuBrowa, FEMA

A barragem Big Tujunga está em obras, para reforçar os muros devido a um aumento no fluxo de detritos causado por fortes tempestades, La Canada Flintridge, Califórnia, 02 Ago 10.

seria considerar a perda de função e a interrupção na geração de eletricidade, ignorando o possível efeito ambiental de um "*tsunami*" no interior. Isso é especialmente preocupante em locais onde há grande densidade populacional e de indústrias ao longo de um rio, como nos Estados da Pensilvânia e da Virgínia Ocidental e em outras áreas onde as cidades cresceram no entorno de moinhos históricos. Caso o ataque cibernético ocorra durante chuvas torrenciais, quando as barragens já estiverem sobrecarregadas, qualquer aumento rápido no nível de água poderá desencadear colapsos sucessivos[8]. Por sua vez, isso poderá levar a uma perda catastrófica de vidas e propriedade, bem como uma perda crítica na capacidade hidrelétrica. Os efeitos ambientais podem ser drásticos e de longo prazo: os recursos de água doce podem ser contaminados; ecossistemas inteiros podem ser destruídos; agentes tóxicos podem ser liberados; e o solo pode sofrer forte erosão ou ser totalmente removido. Cardumes podem ser dizimados, assim como a indústria pesqueira que deles dependem. Os efeitos de curto e longo prazo seriam consideráveis, e os esforços de restauração poderiam ser caros demais para o país. Os danos ambientais seriam permanentes.

Indústria Química dos EUA

A considerável indústria química norte-americana oferece outro exemplo do potencial impacto ambiental de um ataque cibernético. Indústrias manufatureiras e depósitos armazenam grandes quantidades de produtos químicos industriais. A indústria química norte-americana produziu US$ 759 bilhões em produtos químicos em 2011[9]. Mais de 96% de todos os produtos fabricados nos EUA dependem de insumos químicos. Os EUA produzem 15% dos produtos químicos no mundo e transportam, anualmente, 847 milhões de toneladas desses produtos em ferrovias, rodovias e navios de carga[10]. As vias de transporte são adjacentes a riachos, rios, aquíferos subterrâneos, áreas urbanas e terras agrícolas. Uma vez liberados, esses fluidos químicos podem resultar em uma contaminação que exija a mitigação de longo prazo e a restauração e a remediação das áreas afetadas, gerando custos tão altos quanto os observados em locais sendo recuperados com verbas do programa Superfund da Agência de Proteção Ambiental dos EUA (*Environmental Protection Agency — EPA*)[11].

Substâncias químicas podem infiltrar o lençol freático, tornando-o nocivo à saúde; poluir o ar; contaminar o solo; e tornar a terra inadequada para a habitação, agricultura e urbanização. Os danos podem ser irreversíveis caso a defesa cibernética nacional falhe.

Defesa Ambiental

Defender a infraestrutura norte-americana contra ataques cibernéticos não só protege informações, a disponibilidade das redes ou a rede mundial de informações. Também protege as vidas de cidadãos e a propriedade e preserva

ecossistemas e serviços relacionados, dos quais dependemos. Um ataque que leve a danos ambientais pode afetar nossa estabilidade social[12].

A defesa cibernética nacional organizada pelo Departamento de Defesa e outras agências governamentais inclui uma missão "verde", ou ambiental, destinada a garantir que os ataques cibernéticos não produzam danos ambientais irreversíveis dentro dos EUA. Uma efetiva defesa cibernética minimiza o risco de danos significativos às fontes internas de água potável, aos ecossistemas aquáticos e terrestres adjacentes e à biodiversidade. Essa missão deve continuar a proteger os recursos naturais essenciais à vida.***MR***

REFERÊNCIAS

1. OBAMA, Barrack; PANETTA, Leon E. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, Vol. 1 (Washington DC: Government Printing Office, 2012).

2. PANETTA, Leon E. "Defending the Nation from Cyber Attack" (discurso à organização Business Executives for National Security, Nova York, 11 out. 2012).

3. RID, Thomas. "Cyber War Will Not Take Place", *Journal of Strategic Studies* 35, no. 1 (2012): 5-32.

4. RID, Thomas; MCBURNEY, Peter. "Cyber-Weapons", *The RUSI Journal* 157, no. 1 (2012): p. 6-13.

5. Idaho National Laboratory, 2005, "US-CERT Control Systems Security Center", Cyber Incidents Involving Control Systems, INL/EXT-05-00671. Disponível em: <http://www.inl.gov/technicalpublications/documents/3480144.pdf>.

6. KALLBERG, Jan; LOWTHER, Adam. "The Return of Dr. Strangelove", *The Diplomat,* 20 Aug. 2012.

7. LYNN III, William F. "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs* 89 (2010): p. 97.

8. "Isaac Leaves Hundreds of Homes Underwater; Dam Shows Stress", *Los Angeles Times*, 30 Aug. 2012. Disponível em: <http://articles.latimes.com/2012/aug/30/nation/ la-na-isaac-storm-20120831>.

9. American Chemistry Council, <http://www.americanchemistry.com/Jobs/ EconomicStatistics/Industry-Profile/Global-Business-of-Chemistry>.

10. American Chemistry Council, <http://www.americanchemistry.com/ chemistry-industry-facts>.

11. EPA. Superfund Sites, <http://www.epa.gov/superfund/sites/npl/where.htm>.

12. KALLBERG, Jan; THURAISINGHAM, Bhavani. "State Actors's Offensive Cyber Operations-The Disruptive Power of Resourceful Systematic Cyber Attacks", *IEEE IT Professional* 15, no. 3 (2013): p. 32-35.