A guerra cibernética e o vírus Stuxnet

Trata-se do uso da força?

Vinícius Chitolina[*]

Introdução

Um dos principais problemas que encontramos em qualificar e quantificar ataques cibernéticos dentro do contexto do recurso à guerra, que seria o que motiva um país à guerra, ou o também chamado uso da força (como denominado na Carta das Nações Unidas), é a falta de literatura e manuais existentes sobre o assunto. Além disso, a regulação do escopo que a própria Carta de São Francisco (outro nome dado ao acordo que formou a Organização das Nações Unidas – ONU) nos dá não engloba ainda ataques cibernéticos para esses fins. Talvez, isso se deva ao fato de o tema ser relativamente novo e estar sob intenso debate ao redor do mundo.

Um ataque cibernético pode ser definido como qualquer ação direcionada a redes ou qualquer outro meio de comunicação (ZIOLKOWSKI, 2012), podendo ser perpetrado por atores estatais e não estatais. De qualquer modo, a definição se ele pode ser considerado como uso da força ou um recurso ou arma da guerra ainda não está bem determinada. A definição ainda é, de certa forma, nebulosa.

O objetivo deste artigo é analisar se ataques cibernéticos podem ser enquadrados como uso da força segundo o que regulamenta a Carta das Nações Unidas, gerando assim o direito à legítima defesa por parte do atacado, por exemplo. Levou-se em consideração o "Critério Schmitt" para esta análise. O artigo visa checar se o ataque com o vírus Stuxnet pode ser considerado neste contexto.

Este tema é relevante tendo em vista a crescente importância dada ao assunto em vários países ao redor do mundo, os quais têm investido bilhões de dólares em defesa cibernética (SPUTNIK BR, 2017) depois de terem sofrido diversas ações cibernéticas em seus *sites* na internet — como, por exemplo, os sofridos pelos países da Organização do Tratado do Atlântico Norte (OTAN), durante a guerra de Kosovo (NATO REVIEW, 2017).

Vive-se em um mundo imerso em tecnologia e sendo guiado para o que se chama de "Internet das Coisas". Estima-se que até 2020 haverá cerca de 50 bilhões de dispositivos conectados na internet (ALECRIM, 2016). Portanto torna-se importante o objetivo deste artigo, baseando-se na Carta da

---

[*] 2º Ten Com (AMAN/17). Apresentou o tema no simpósio internacional Civil-Military Cooperation and International Collaboration in Cyber Operations (Universidade do Norte da Geórgia - EUA/17). Atualmente, é Cmt Pel no 1º Batalhão de Guerra Eletrônica.

Organização das Nações Unidas, mais precisamente no Artigo 2, inciso 4.

Na **Figura 1**, verificamos a grandiosidade do que se chama Internet das Coisas, onde haverá uma imensa superfície de ataque para ações cibernéticas.

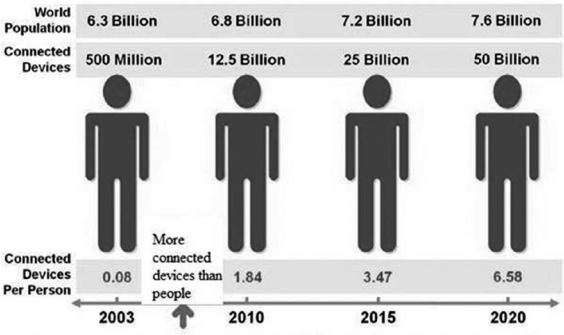

Figura 1 – Internet das Coisas
Fonte: Cisco IBSG[1]

A hipótese é a seguinte: os ataques cibernéticos podem ser enquadrados como uso da força, de acordo com as suas características e com a Carta de São Francisco.

Desenvolvimento

Metodologia

Foi desenvolvida uma pesquisa bibliográfica. As principais referências foram: a própria Carta da Nações Unidas, mais precisamente o Artigo 2, inciso 4; o *Manual Tallinn em Operações Cibernéticas*; e a opinião de especialistas no assunto, como Michael N. Schmitt (MICHAEL, 2013).

Fundamentação teórica

O trabalho baseou-se primordialmente na própria Carta de São Francisco da ONU, que teve como objetivo transferir o monopólio da força legítima de cada Estado para um gendarme mundial. Muitas vezes legitimando guerras e atos hostis.

Sustentou-se também na Regra 11 do *Tallinn Manual on the International Law Applicable to Cyber Warfare*, que versa sobre a aplicabilidade da lei internacional na resolução de "ciberconflitos". Mais especificamente, no *jus ad bellum* (dita sobre as razões aceitáveis para um país entrar em guerra) e no *jus in bello* (regula as condutas aceitáveis nos conflitos armados).

O Artigo 2, inciso 4 da Carta da Organização das Nações Unidas, afirma que:

> Todos os membros deverão evitar em suas relações internacionais a ameaça ou o uso da força contra a integridade territorial ou a dependência política de qualquer Estado, ou qualquer outra ação incompatível com os Propósitos das Nações Unidas. (NAÇÕES UNIDAS, 1945)

A Regra 11 do *Tallinn Manual on the International Law Applicable to Cyber Warfare*, do qual provém o "Critério Schimitt" para análises de uso da força, afirma que, para se afirmar se a ação pode ser considerada uso da força, devemos responder a uma série de perguntas as quais são encontradas no próprio manual (transcrição não literal, adaptada e traduzida para o Português):

> Fatores propostos que influenciam assertivas sobre o uso da força (não é um critério formal). Severidade: quantas pessoas morreram? Quão grande foi a área afetada? Imediaticidade: quão breve foram sentidos os efeitos da operação cibernética? Diretividade: a ação tem proximidade com os efeitos causados? Invasividade: a ação cibernética penetrou em uma rede que deveria ser segura? Foi o *locus* da ação o país atingido? Mensurabilidade dos efeitos: como os efeitos podem ser quantificados? Os efeitos são uma ação distinta ou provém de ações paralelas? Caracterização

> militar: a ação foi conduzida por militares? Envolvimento estatal: o Estado está diretamente ou indiretamente envolvido na ação em questão? Presunção de legitimidade: essa ação pode ser caracterizada como uso da força, ou não pode ser caracterizada como uso da força? (MICHAEL, 2013)

O critério acima exposto é de suma importância para o desenvolvimento do artigo, tendo em vista ser utilizado para a verificação se uma ação cibernética é cabida no contexto de uso da força. A qualificação da ação sob égide da ONU iria legitimar ou não uma ação cibernética. O trabalho desenvolveu-se em cima desses dois documentos, procurando verificar e analisar a ação do vírus Stuxnet e suas consequências.

Analisando o vírus Stuxnet pelo "Critério Schmitt"

O vírus Stuxnet pode ser considerado como um divisor de águas, podendo ser definido como um dos primeiros ataques cibernéticos em tempos de paz. De acordo com reportes, o vírus foi especificamente desenvolvido para atingir instalações nucleares no Irã, atrasando em anos o programa nuclear iraniano.

Na **Figura 2**, verificamos a porcentagem de máquinas infectadas por país, e verifica-se que grande parte dos ataques se direcionou para o Irã, país onde estavam as usinas nucleares, que eram os alvos dos ataques.

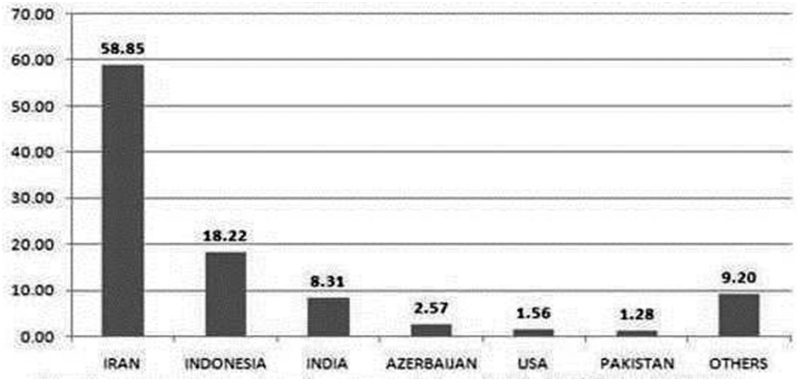

Figura 2 – Porcentagem de ataques do vírus Stuxnet por países
Fonte: www.symantec.com[2]

Severidade: considerando este critério, o Stuxnet pode ser considerado como uso da força, em razão dos severos danos cinéticos causados às instalações nucleares do Irã.

Imediaticidade: o ataque levou considerado tempo para atingir seu alvo, demorou certo tempo para ser descoberto, então não pode ser considerado como uso da força.

Diretividade: há ligação direta do vírus Stuxnet com a danificação das centrífugas, então pode ser considerado como uso da força. "Os principais alvos do vírus são sistemas de controle de automação e monitoramento industrial, conhecidos pela sigla SCADA" (ROHR, 2011).

Invasividade: foi extremamente invasivo, uma significante intrusão na soberania iraniana, que atingiu uma rede não conectada na rede mundial de computadores e um sistema extremamente seguro. Logo, pode ser considerado como uso da força.

> Cada tipo de usina de enriquecimento de urânio usa esse sistema numa configuração particular. E o vírus foi programado para atacar só a configuração que as usinas do Irã usam. (VERSIGNASSI, 2011)

Mensurabilidade: houve uma considerável taxa de falha nas centrífugas, logo pode ser considerado como uso da força.

> Foi nessas centrífugas que foi testada a eficiência do *worm* Stuxnet, *malware* de computador que teria danificado cerca de um quinto das centrífugas iranianas. (TEIXEIRA, 2011)

Caracterização militar: não há evidências que comprovem engajamento militar no ataque, até mesmo devido à própria natureza de ações cibernéticas, onde há uma grande dificuldade de verificar de onde o ataque surgiu, então, não pode ser considerado uso da força se baseando nesse aspecto.

Envolvimento estatal: não há evidências de que houve um país envolvido no ataque, mas, pelas marcáveis características do vírus, há a possibilidade de algum envolvimento estatal; contudo, no caso, o Stuxnet não pode ser considerado uso da força.

> O *malware* Stuxnet reconhecidamente foi a mais sofisticada "ciber-arma" já desenvolvida e aparentemente foi uma obra conjunta de diversos autores espalhados em vários continentes. (TEIXEIRA, 2011)

Presunção de legitimidade: no uso do Stuxnet, não há presunção de legitimidade, devido ao fato de a ação não ter sido desencadeada com propósitos de autodefesa, nem autorizado pelo Conselho de Segurança da Organização das Nações Unidas. E, até mesmo nestes casos, pode ser considerado como não amparado, ou fora da regulamentação, considerando que não há qualquer consentimento da comunidade internacional em ataques que causem danos a instalações nucleares de outros Estados.

Baseando-se nessas assertivas, nós podemos concluir que muitos estados provavelmente considerariam o vírus Stuxnet como sendo uso da força, principalmente pelas suas características únicas e sua severidade, a qual destruiu cerca de mil reatores nucleares (SHUBERT, 2011).

Os critérios acima adotados para a análise são subjetivos, cabendo a cada Estado a aplicabilidade deles. Eles servem como um direcionamento para que, no futuro, possa ser definido de maneira mais clara e objetiva as ações cibernéticas que podem ou não ser consideradas como arma de guerra e uso da força.

Conclusão

Esta pesquisa visou analisar o uso da força em ataques cibernéticos, de acordo com o "Critério Schmitt". Assumindo que ataques cibernéticos podem ser considerados como uso da força, nós aplicamos esses critérios para analisar o ataque do vírus Stuxnet, com a intenção de classificá-lo como uso da força, se aplicável.

A hipótese de que ataques cibernéticos podem ser considerados como uso da força foi parcialmente confirmada, devido às dificuldades em qualificar o contexto do ataque como uso da força, devido às diversas variáveis que o envolvem.

Apesar da dificuldade de se definir a origem do ataque, mensurar os efeitos cinéticos e a severidade da ação, o "Critério Schmitt" provou ser uma importante ferramenta para analisar o uso da força em ataques cibernéticos. Principalmente, devido ao fato de que muitas vezes os ataques cibernéticos não destroem, mas somente desabilitam ou roubam informações do alvo em questão, podendo ser muito mais danosos que a destruição propriamente dita.

Finalmente, a análise realizada indica que seria importante expandir o escopo do Artigo 2, inciso 4 da Carta da Organização das Nações Unidas, que apresenta uma visão estrita do que pode ser considerado como uso da força. Especialmente quando nós levamos em consideração as características do espaço cibernético, onde uma ação simples e de baixo custo pode gerar um grave efeito destrutivo. REB

Referências

ALECRIM, Emerson, **O que é Internet das Coisas (Internet of Things)?** 2016. Disponível em: <www.infowester.com/iot.php>. Acesso em: 3 de novembro de 2017.

MICHAEL N. Schmitt, **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge, NY: Cambridge, 2013.

NATO REVIEW. **New threats: the cyber-dimension.** Disponível em: <www.nato.int/docu/review/2011/11-september/Cyber-Threads/EN/index.htm>. Acesso em: 1º de novembro de 2017.

NAÇÕES UNIDAS, **Carta das Nações Unidas.** San Francisco, CA: UN, 1945.

ROHR, Altieres. **Saiba como age o vírus que invadiu usinas nucleares no Irã e na Índia.** 2010. Disponível em: <g1.globo.com/tecnologia/noticia/2010/10/saiba-como-age-o-virus-que-invadiu-usinas-nucleares-no-ira-e-na-india.html>. Acesso em: 2 de novembro de 2017.

SHEARER, Jarrad. **W32.Stuxnet.** Disponível em: <www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99>. Acesso em: 3 de novembro de 2017.

SHUBERT, Atika. **Cyber warfare: A different way to attack Iran's reactors.** 2011. Disponível em: <edition.cnn.com/2011/11/08/tech/iran-stuxnet/index.html>. Acesso em: 2 de novembro de 2017.

SPUTNIK BR. **Segurança cibernética e satélites custarão à otan 3 bilhões de euros.** Disponível em: <sptnkne.ws/dUQw>. Acesso em: 1º de novembro de 2017.

TEIXERA, Carlos Alberto. **Vírus Stuxnet, que atacou usinas nucleares no Irã, foi criado em parceria por EUA e Israel.** 2011. Disponível em: <oglobo.globo.com/sociedade/tecnologia/virus-stuxnet-que-atacou-usinas nucleares-no-ira-foi-criado-em-parceria-por-eua-israel-2836696>. Acesso em: 2 de novembro de 2017.

VERSIGNASSI, Alexandre. **Vírus entra em programa nuclear e salva o mundo.** 2011. Disponível em: <super.abril.com.br/tecnologia/virus-entra-em-programa-nuclear-e-salva-o-mundo/>. Acesso em: 2 de novembro de 2017.

ZIOLKOWSKI, Katharina. **Ius ad bellum in Cyberspace – Some Thoughts on the "Schmitt-criteria" for Use of Force**, Tallinn, EE: NATO, 2012.

N. da R.: A adequação do texto e das referências às prescrições da Associação Brasileira de Normas Técnicas (ABNT) é de exclusiva responsabilidade dos articulistas.

---

[1] www.nonlinearthinkingblog.com/nonlinear_thinking/internet-of-things/ (abril de 2011).
[2] www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.