ARTIGO CIENTÍFICO
ÁREA DE CONCENTRAÇÃO

CIBERNÉTICA

A GUERRA CIBERNÉTICA E O VÍRUS STUXNET: TRATA-SE DE USO DA FORÇA?

Vinícius Chitolina
Graduado em Ciências Militares

RESUMO: Um ataque cibernético pode ser definido como uma ação direcionada a redes ou qualquer outro meio de comunicação e informação, podendo ser considerados atores estatais e atores não estatais. Contudo, o fato de essas ações serem consideradas como uso da força segundo a cartilha da Organização das Nações Unidas ainda é um ambiente nebuloso, ou seja, não há definições exatas. O objetivo desse artigo é analisar o uso da força em ataques cibernéticos. Levando em consideração o "Critério de Schmitt" para análise, o artigo visa verificar se o vírus Stuxnet pode ser classificado como tal. Uma possível hipótese é que ataques cibernéticos podem ser considerados uso da força, segundo o que normatiza a própria cartilha da Organização das Nações Unidas. Esta análise indicará que poderia importante ser ampliado o escopo do artigo 2 inciso 4 da cartilha da ONU, a qual apresenta uma estrita visão do que seria considerado uso da força, especialmente quando levamos em consideração o espaço cibernético, onde uma simples ação de pequeno custo pode causar um dano gigantesco. Além disso, o "Critério de Schmitt" provou ser uma importante ferramenta para analisar o uso da força em ataques cibernéticos, mesmo com diversos problemas como a origem da ação, a mensurabilidade dos efeitos cinéticos do ataque a e severidade da ação que se faz difícil de determinar. Muitas das vezes ataques cibernéticos não destroem o objetivo, mas somente danificam ou roubam informações do alvo, e consequentemente os efeitos podem ser muito piores que a destruição. A hipótese que os ataques cibernéticos podem ser considerados como uso da força foi parcialmente confirmada, tendo em vista a dificuldade em qualificar no contexto do ataque o uso da força, devido as várias variáveis que o envolvem.

Palavras-chave: Analisar. Ataque Cibernético. Escopo. Stuxnet. Uso da força

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 e também a regulação do escopo que a própria Carta de São Francisco (outro nome dado ao acordo que formou a Organização das Nações Unidas) nos dá, que não engloba ainda ataques cibernéticos para estes fins, podemos atribuir isso 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 considerados atores estatais e não estatais. De qualquer modo, a definição se ele pode ser verificado como uso da força, ou um recurso ou arma da guerra ainda não foi bem definido, o ambiente ainda é de certa forma nebuloso.

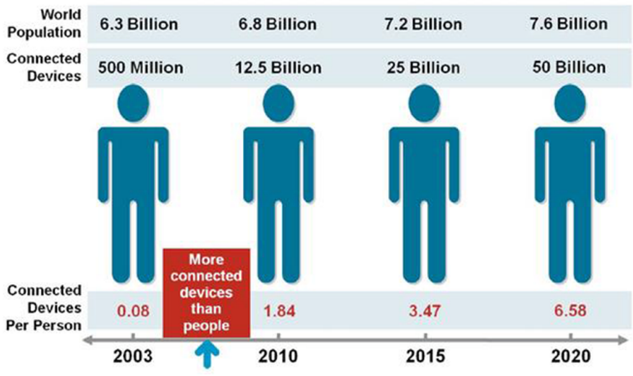
O objetivo desse artigo é analisar se ataques cibernéticos podem ser enquadrados como uso da força segundo o que regulamenta a Carta das Nações Unidas, gerando assim o direito à legítima defesa por parte do atacado, por exemplo. Levou-se em consideração o "Critério Schmitt" para esta análise. O artigo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

Esse 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 ter sofrido diversas ações cibernéticas em seus

sites na internet – como por exemplo os sofridos pelos países da Organização do Tratado do Atlântico Norte, 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, a qual estima-se que até 2020 haverá cerca de 50 bilhões de dispositivos conectados na internet (ALECRIM, 2016). Portanto, faz-se importante o desenvolver deste artigo, baseando-se na Carta da Organização das Nações Unidas, mais precisamente no Artigo 2, inciso 4.

FIGURA 1 Gráfico Comparativo População Mundial x Dispositivos Conectados



Fonte: Cisco IBSG, 2011.

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

1 METODOLOGIA

Foi desenvolvida uma pesquisa bibliográfica. Nossas maiores referências são: a própria Carta da Nações Unidas, mais precisamente o artigo 2, inciso 4; o Manual Tallinn em Operações Cibernética; e a opinião de especialistas no assunto como Michael N. Schmitt (MICHAEL, 2013).

2 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 o jus in bello (regula as condutas aceitáveis nos conflitos armados).

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

> "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)

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

racterizada como uso da força, ou não pode ser caraterizada como uso da força? (MICHAEL, 2013).

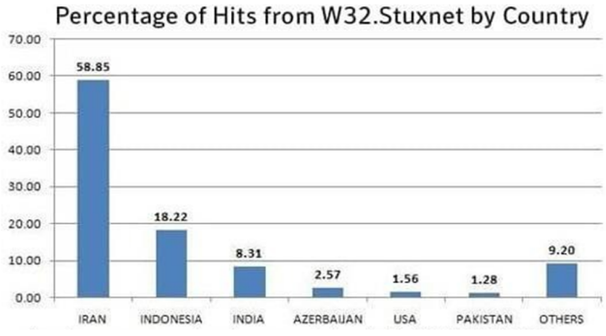
O critério acima exposto é de suma importância para o desenvolvimento do artigo, tendo em vista ser utilizado para a verificação se uma ação cibernética é cabida no contexto de uso da força. E a qualificação da ação, sob égide da ONU, iria legitimar ou não uma ação cibernética. O trabalho desenvolveu-se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

3 ANALISANDO O STUXNET VÍRUS PELO "CRITÉRIO SCHMITT". FUNDAMENTAÇÃO TEÓRICA

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 abaixo verificamos a porcentagem de máquinas infectadas por país, e verifica-se que grande parte dos ataques se direcionaram para o Irã, país onde estavam as usinas nucleares alvo dos ataques.

FIGURA 2 Porcentagem de máquinas infectadas por país



Fonte: Symantec, 2017

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

Imediatividade: 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: o uso do Stuxnet não há presunção de legitimidade, devido a ação não ter sido desencadeada devido a propósitos de auto defesa 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. Tais critérios servem como um direcionamento para que no futuro possam ser definidas, de maneira mais clara e objetiva, as ações cibernéticas que podem ou não serem 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 confirmado, devido às dificuldades em qualificar o contexto do ataque como uso da força, dado as diversas variáveis que o envolvem.

Apesar de tudo isso, o “Critério Schmitt” provou ser uma importante ferramenta para analisar o uso da força em ataques cibernéticos. Entretanto, problemas tais como: definir a origem do ataque; a mensurabilidade dos efeitos cinéticos; e a severidade da ação;

dificultam essa análise. Isso se deve, principalmente, ao fato de que muitas vezes os ataques cibernéticos não destroem, mas tão somente desabilitam ou roubam informações do alvo em questão, e os efeitos podem ser muito mais danosos do 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 poder de destruição.

THE CYBER-WAR AND THE STUXNET VIRUS: IS IT A USE OF FORCE?

ABSTRACT: A cyber-attack could be defined as some action directed to networks or any other means of communication and information considering state actors and non-state actors. However, whether this should be seen as use of force is still undetermined. This article's objective is to analyze the use of force in cyber-attacks. Taking into account the "Schmitt Criteria" for analysis, it aims at checking if the Stuxnet virus attack could be classified as it. The hypothesis is that cyber-attacks can be considered according to the UN Charter due to its characteristics. The analysis indicated that it would be important to expand the scope of the Article 2(4) UN Charter, which presents a strict view of what may be considered use of force. Especially when we take into account the cyberspace, where a simple and low cost action can have a great power of destruction. Although "Schmitt Criteria" proved to be an important tool to analyze the use of force in cyber-attacks, issues such as the origin of the attack, the measurement of the kinetic effects and severity of the action were difficult to determine. Mainly because sometimes a cyber-attack do not destroy but only disable or steal information from the target, and the effects of it may be even worse than the destruction. The hypothesis that the cyber-attacks could be considered use of force was partially confirmed, because of the difficulties in qualifying the context of the attack as use of force, due to the many variables involved in it.

Keywords: Analyze. Cyber-Attack. Stuxnet. Use of Force.

REFERÊNCIAS

ALECRIM, Emerson, O que é Internet das Coisas (Internet of Things)? 2016. Disponpivel em: . 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 . Acesso em: 1 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: . Acesso em 2 de novembro de 2017.

SHUBERT , Atika. Cyber warfare: A different way to attack Iran's reactors. 2011. Disponível em . Acesso em 2 de novembro de 2017.

SPUTNIK BR. Segurança cibernética e satélites custarão à otan 3 bilhões de euros. Disponível em . Acesso em: 1 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: . Acesso em 2 de novembro de 2017;

VERSIGNASSI, Alexandre. Vírus entra em programa nuclear e salva o mundo. 2011.Disponível em: . 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

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras – Resende – RJ. Atualmente, está servindo no 1° Batalhão de Guerra Eletrônica e pode ser contactado pelo email: chitolina.vinicius@eb.mil.br.