XIX encontro nacional de pesquisa em ciência da informação
ENANCIB
// SUJEITO INFORMACIONAL E AS PERSPECTIVAS ATUAIS EM CIÊNCIA DA INFORMAÇÃO. //
22-26 OUTUBRO 2018
LONDRINA/PR
Universidade Estadual de Londrina

XIX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2018

GT- 8 – Informação e Tecnologia - Pôster

CIBERTERRORISMO NA PARAÍBA

Wagner Junqueira de Araújo (Universidade Federal da Paraíba - UFPB)

José Roberto Cavalcante da Silva (Universidade Federal da Paraíba - UFPB)

CIBERTERRORISM IN PARAÍBA

Modalidade da Apresentação: Pôster

Resumo: Nos últimos anos houve um aumento significativo da ocorrência de ataques virtuais em todo o mundo. Estes ataques acontecem na forma de invasões maliciosas, suspensão temporária de serviços, violação de dados, atividades de espionagem, sequestro de informações, etc. Neste ambiente instável, grupos terroristas passaram a explorar o espaço cibernético de maneira célere, como mais um canal para disseminar suas mensagens, criando insegurança e medo. Esta pesquisa teve como objetivo estudar o ciberterrorismo na Paraíba por meio de cenários prospectivos. A amostra foi do tipo intencional por conveniência, composta por órgãos públicos e empresas privadas que sofreram ataques ou ameaças de ataques descritas na mídia local relacionadas com o ciberterrorismo no período de janeiro de 2016 até o final de 2017. Para análise dos dados foram aplicados: a análise estrutural; o método de atores; identificação de objetivos; análise de relações de força; e a análise morfológica. Com base nas análises desenvolvidas junto às variáveis e atores, foram descritos três cenários possíveis relacionados com o ciberterrorismo: cenário propício; cenário adverso; e um cenário provável. Foi identificado que o ator "governo" exerce forte influência nos demais, sendo responsável pelas variações dos cenários. Entre os resultados foi verificado que as organizações estão cientes da ameaça do ciberterrorismo, mas se mostram inertes a este tipo de ameaça, sem implementar nenhum tipo de ação ou política específica de segurança da informação.

Palavras-Chave: Gestão da Segurança da Informação; Tecnologias da Informação e da Comunicação; Ciberterrorismo; Cenários Prospectivos.

Abstract: In recent years there has been a significant increase in the occurrence of cyber attacks worldwide. These attacks happen in the form of malicious intrusions, temporary suspension of services, data breaches, espionage activities, hijacking of information, etc. In this unstable environment, terrorist groups began to explore cyberspace quickly, as another channel to disseminate their messages, creating insecurity and fear. This research aimed to study cyberterrorism in Paraíba

using prospective scenarios. The sample was intentional type of convenience formed by public agencies and private companies that have suffered attacks or threats of attacks described in the local media concerning cyberterrorism in January 2016 period to the end of 2017. For data analysis were applied: structural analysis; the actor method; identification of objectives; analysis of force relationships; and morphological analysis. Based on the analysis developed with the variables and actors were described three possible scenarios related to cyber terrorism: setting conducive; adverse scenario; and a probable scenario. It was identified that the actor "government" strongly influence others, being responsible for changes in the scenarios. Among the results it was found that organizations are aware of the threat of cyberterrorism, but show inert to this type of threat, without implementing any action or specific policy information security.

Keywords: Information Security Management; Information and Communication Technologies; Cyber Terrorism; Prospective Scenarios.

1 INTRODUÇÃO

Na última década houve um aumento significativo da ocorrência de ataques virtuais em todo o mundo. O relatório da PWC (2016) em sua 18ª edição "*A Global State of Information Security*", apresenta um crescimento exponencial nos incidentes de informação a nível mundial, e indica um crescimento de 274% de números de ataques cibernético no Brasil, estes números são corroborados pelas estatísticas disponíveis no portal do Cert.br (2016).

Ataques acontecem na forma de invasões maliciosas, suspensão temporária de serviços, violação de dados, atividades de espionagem, sequestro de informações, etc. Neste ambiente instável, grupos terroristas passaram a explorar o espaço cibernético de maneira célere como mais um canal para disseminar suas mensagens, criando um ambiente de insegurança e medo (ALBAHAR, 2017). Dentre os diferentes tipos de ataques, um chama atenção, o que realiza sequestro de informações em formato digital.

Conforme estes grupos evoluem no ciberespaço, a Gestão de Segurança da Informação - GSI tem sua atuação dificultada, pois está diante de novas ameaças, como: ciberativismo e o ciberterrorismo. Essas ameaças apresentam em comum a realização de ataques contra computadores por meio do ciberespaço, contudo sua intenção ou motivação diferem. Neste estudo, o objeto será o fenômeno do terrorismo cibernético ou ciberterrorismo.

O terrorismo cibernético é uma ameaça em desenvolvimento no século XXI, tornando a gestão da segurança da informação em ambientes cibernéticos ainda mais crítica. Tais ameaças apresentam riscos potenciais, porém ainda não é possível encontrar uma definição ou padrões comuns, o que prejudica a tomada de decisão do gestor de segurança da informação em relação aos ataques de ciberterroristas (ALBAHAR, 2017).

Diante dessas exposições, este estudo buscou responder à seguinte questão de pesquisa: quais são os cenários sobre o ciberterrorismo na Paraíba? O objetivo proposto foi estudar o ciberterrorismo na Paraíba por meio de cenários prospectivos.

O ciberterrorismo é um evento de difícil definição. Isso dificulta alcançar uma boa solução para combatê-lo. Gordon e Ford (2002) indicam alguns tipos de ciberterrorismo: o legítimo; terrorismo como teatro; e o novo terrorismo. O primeiro são os ataques praticados contra computadores, redes e informações inseridas nos computadores, ou seja, são as atividades de terrorismo que são executadas integralmente no ciberespaço, em que só o computador é o alvo. O segundo pode ser compreendido como uma metáfora, posto que os incidentes terroristas são simulados através de sites próprios dos grupos terroristas. Esses sites são utilizados para solicitar dinheiro, divulgar mensagens, promover a sua causa e recrutar novos terroristas. O novo terrorismo, por sua vez, acontece com o apoio das organizações terroristas financiadas. São grupos tecnologicamente estruturados, apresentando capacidade de causar danos avassaladores a um amplo conjunto de alvos. Nesse sentido, não são apenas as informações contidas nos computadores o foco dos ataques, mas também áreas de infraestrutura que se utilizam do espaço virtual (GORDON; FORD, 2002).

Em relação à intenção dos ataques cibernéticos, nota-se que as motivações são diversas, sendo que as com propósito de obter vantagem financeira e as de cunho ideológico são as que mais se enquadram como ações ciberterroristas. O quadro 1 descreve algumas destas motivações para ataques virtuais.

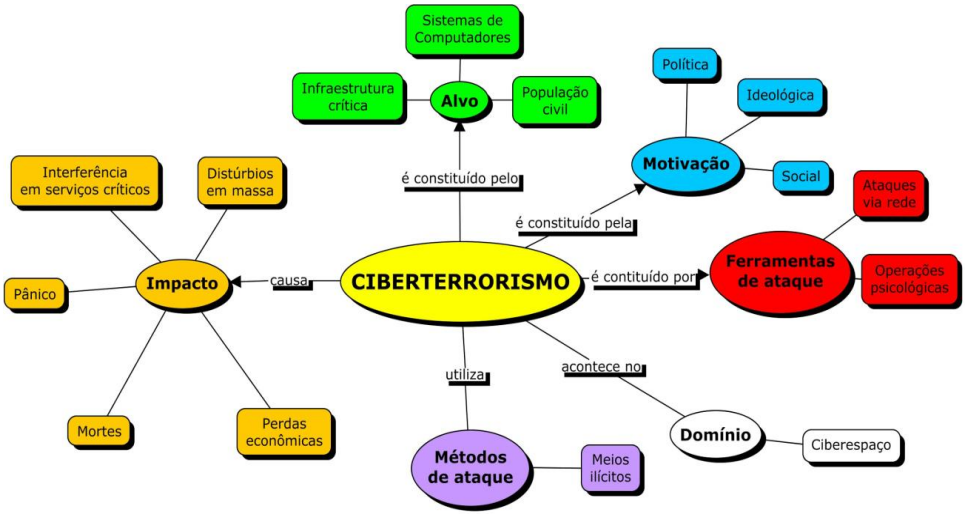
Quadro 1 - Motivos dos ataques cibernéticos

Motivo	Descrição
Demonstração de poder	mostrar a uma empresa que ela pode ser invadida ou ter os serviços suspensos e, assim, tentar vender serviços ou chantageá-la para que o ataque não ocorra novamente.
Prestígio	vangloriar-se, perante outros atacantes, por ter conseguido invadir computadores, tornar serviços inacessíveis ou desfigurar *sites* considerados visados ou difíceis de serem atacados.
Motivações financeiras	coletar e utilizar informações confidenciais de usuários para aplicar golpes.
Motivações ideológicas	tornar inacessível ou invadir *sites* que divulguem conteúdo contrário a opinião do atacante; divulgar mensagens de apoio ou contrárias a uma determinada ideologia.
Motivações comerciais	tornar inacessível ou invadir *sites* e computadores de empresas concorrentes, para tentar impedir o acesso dos clientes ou comprometer a reputação destas empresas.

Fonte: Adaptado de CERT.br (2016, p. 17-18).

Ahmad *et al.* (2012) afirmam que é relevante perceber as semelhanças e as diferenças acerca do que se constitui o terrorismo cibernético, permitindo assim elaborar políticas para o combate dessa ameaça. Os autores sugerem que os seguintes elementos compõem o tema: alvo (sistemas de computadores, infraestrutura crítica, população civil); motivação (política, ideológica, social); ferramentas de ataque (ataques via rede, operações psicológicas); domínio (ciberespaço); métodos de ataque (meios ilícitos); e impacto (distúrbios em massa ou interferência em serviços críticos, pânico, mortes, perdas econômicas). A figura 1 apresenta um mapa com esses elementos.

Figura 1 - Elementos do Ciberterrorismo



Fonte: Elaborado pelos autores, com base em Ahmad *et al.* (2012).

No período de maio a agosto de 2015, os principais incidentes foram os *Ransomware* e *Stagefright*. O primeiro age como um sequestrador de informações em arquivos digitais. Nesse golpe, as informações sequestradas são cifradas e a vítima é conduzida ao pagamento de um resgate através de transferência bancária ou por meio de moeda virtual (*bitcoins)*. O segundo trata de uma vulnerabilidade no Android (RNP, 2015). No primeiro semestre de 2017, o *Ransomware* voltou a ser destaque, pois nesse período um ataque causou uma das maiores crises virtuais de nível global, provocando no Brasil grandes prejuízos em órgãos públicos, empresas do setor privado e em instituições da rede de ensino e pesquisa (RNP, 2017).

2 DESENVOLVIMENTO

Esta pesquisa apresenta uma natureza qualitativa-quantitativa, pois quantificou os dados coletados, analisando-os de forma qualitativa. Além disso, a pesquisa pode ser

classificada em bibliográfica quanto aos meios e descritiva quantos aos fins. Para a identificação das variáveis e dos atores, foi realizado levantamento bibliográfico por meio de consultas no Portal de Periódicos CAPES, em que foram usados os seguintes termos chaves na língua portuguesa: ciberterrorismo e ciberativismo, e os termos chaves em língua Inglesa: *cyberterrorism e cyberactivism*, além outras fontes de pesquisa bibliográficas.

A amostra foi do tipo intencional por conveniência, composta por indivíduos do setor de tecnologia da informação e comunicação de oito organizações na Paraíba que se disponibilizaram a participar da pesquisa. Estas organizações foram citadas na mídia local, nos ataques de 2015 e 2017. Foram consultados 16 (dezesseis) participantes, 12 (doze) servidores públicos de seis órgãos distintos, dois colaboradores de uma empresa pública e dois de uma organização privada.

Segundo Godet e Durance (2011) "o método dos cenários visa construir representações dos futuros possíveis, bem como das sequências de acontecimentos que a eles conduzem." (GODET; DURANCE, 2011, p. 48). Este estudo utilizou três etapas principais do método apontadas por Godet (1994): a) delimitação do sistema e do ambiente estudado; b) identificação das variáveis e dos atores; c) construção dos cenários prospectivos possíveis aplicados ao ciberterrorismo na Paraíba. Para a coleta dos dados, foi utilizado um formulário composto por treze questões, incluindo as matrizes de variáveis, atores e objetivos, que foram preenchidos pelos participantes da pesquisa. Para a análise, a descrição e a construção dos cenários, foram empregadas três etapas do método de cenário: a análise estrutural, auxiliada pelo software Matriz de Impactos Cruzados - Multiplicações Aplicadas a uma Classificação (MICMAC); o Método de Atores, Objetivos, Relações de força, auxiliado pelo software MACTOR; e a análise morfológica.

De acordo com a revisão da literatura e do contexto organizacional abordado, foram identificadas as seguintes variáveis: políticas públicas; ideologias; mercado; tecnologias; e vantagem indevida. Para a matriz utilizada na análise estrutural, os participantes preencheram indicando o grau de influência direta de uma variável sobre a outra, atribuindo os seguintes valores: (0) sem influência direta; (1) fraca; (2) média; (3) forte; e (P) potenciais, que podem acontecer em algum momento futuro. Os dados obtidos foram consolidados de forma estatística através da Moda (M_o). Para tanto, substituiu-se o (P) de potenciais por (4) para calcular o valor da M_o. Em seguida, os dados foram transcritos para o software MICMAC,

possibilitando identificar a influência e a dependência das variáveis na forma de gráficos e mapas, que indicaram as relações diretas, indiretas e potenciais das variáveis.

Verificou-se que a variável "vantagem indevida" foi a de maior influência e pouca dependência. Este resultado corrobora com a literatura (AHMAD *et al*., 2012), que relata os últimos ataques com o intuito de obter lucro por meio da cobrança em moeda digital (*bitcoins*). As variáveis "mercado" e "políticas públicas", foram identificadas como de grande influência, mas de maior dependência. Isto indica que, apesar de influenciarem às outras, elas são influenciadas na mesma proporção. As variáveis "tecnologias" e "ideologias", por sua vez, foram classificadas como pouco influentes e muito dependentes. Não foram identificadas variáveis pouco influentes e pouco dependentes.

Os atores e os objetivos também foram determinados segundo a revisão da literatura e do contexto organizacional abordado. Como atores: governo; empresas; colaboradores; clientes/usuários e pessoas externas; e como objetivos: elaborar políticas públicas; divulgar ideologias; propor novas ideias; usar as tecnologias e obter benefícios ilícitos. Na matriz de análise do grau de influência de um ator sobre o outro, os participantes fizeram o preenchimento, atribuindo os seguintes valores: (0) sem influência direta; (1) processos; (2) projetos; (3) missão; e (4) existência. Na matriz que verifica se o objetivo tem consequência sobre o ator, os participantes fizeram o preenchimento atribuindo os seguintes valores: (0) o objetivo é pouco consequente; (1) o objetivo tem consequências sobre os processos do ator; (2) o objetivo tem consequências sobre os projetos do ator; (3) o objetivo tem consequências sobre a missão do ator; e (4) o objetivo tem consequências sobre a existência do ator. Ressalta-se que nessa matriz é necessário indicar se o ator é favorável ou desfavorável ao objetivo. Isso foi realizado por meio da inserção do sinal (+/-) aos números. Os dados coletados foram tabulados de forma estatística por meio da Moda (M_o). Em seguida, os valores da M_o foram transferidos para o software MACTOR, permitindo a análise das relações: atores x atores; objetivos x atores.

Os atores "clientes/usuários", "governo", "colaboradores" e "empresas" foram classificados como atores de ligação, que segundo Godet e Durance (2011) são tão influentes quanto dependentes, ou seja, exercem influência e dependem dos demais atores no contexto estudado. O ator "pessoas externas" foi identificado como um ator autônomo, não sendo influente nem dependente. Não foram identificados atores dominantes, nem atores dominados.

Na análise de convergências: mais fortes; fortes; moderadas; fracas; e mais fracas; verificou-se que os atores "empresas" e "colaboradores" apresentaram uma relação de convergência mais forte, com maior nível de intensidade. Os atores "governo" e "clientes/usuários" dispõem de uma convergência moderada entre si e entre os atores "colaboradores" e "empresas". O ator "pessoas externas", por sua vez, apresentou uma convergência mais fraca em relação a todos os atores deste estudo. Vale ressaltar que em suas falas os participantes destacaram a necessidade de atuação do governo como fomentador de políticas de segurança da informação.

3 APRESENTAÇÃO DOS CENÁRIOS

A prospecção de cenários gera um conjunto de informações estratégicas que podem ser usadas para a tomada de decisão. Com base nas informações criadas, as organizações podem ajustar seus planejamentos estratégicos. No entanto, para Godet e Durance (2011, p. 9-42), cenário não é a realidade futura, mas um meio de representá-la, com vista a esclarecer a ação presente à luz dos futuros possíveis e desejáveis, além de possibilitar a visualização do "campo dos prováveis" na perspectiva estratégica. Com os resultados apurados pelas análises foram elaborados três cenários possíveis.

a) **Cenário propício ao ciberterrorismo**: A partir da relação de convergência mais forte entre os atores "empresas" e "colaboradores". Quando as empresas não fazem investimento em treinamentos e não oferecem uma infraestrutura de tecnologia da informação adequada para seus colaboradores. Reforçado por meio da relação moderada entre do ator "governo" que não fomenta a elaboração de legislações, e normas fragilizando as ações de segurança da informação nas organizações.
b) **Cenário adverso ao ciberterrorismo**: Este cenário pode se constituir quando o ator "governo" passa a criar legislações, normas e os mecanismos de proteção, fomentando a segurança da informação. Por sua vez as empresas realizam investimentos em treinamentos de seus colaboradores e disponibilizam uma infraestrutura de tecnologia da informação adequadas. Estes atores terão ferramentas para cumprir com suas políticas de segurança da informação, realizando constantes treinamentos de seus colaboradores, atualizações de *softwares* e aplicativos.
c) **Cenário provável:** Sem uma atuação continuada na construção de uma legislação específica ou na atualização das legislações existentes e com sua imagem associada à corrupção e atos ilícitos (verificado pelas relações da variável "vantagem indevida"), o governo deixa de fomentar a criação de normas e mecanismos de proteção, desta maneira as "empresas" não atualizam seus recursos de

tecnologia da informação nem preparam seus colaboradores acerca dos princípios básicos da segurança da informação.

A maioria dos participantes entendem que a Gestão da Segurança da Informação é essencial para as organizações contemporâneas. Contudo, os participantes indicaram que suas organizações não estão plenamente preparadas para assegurarem os princípios básicos da segurança da informação. Somente 50% dos participantes responderam que existe uma política de segurança da informação em suas instituições. Os participantes também apontaram que as ameaças involuntárias são as mais comuns, seguidas das voluntárias.

O papel do ator "governo" nos cenários elaborados foi de destaque, pois a maior parte da amostra foi composta por especialistas vinculados a órgãos ou empresas governamentais.

4 CONSIDERAÇÕES

O objetivo proposto foi estudar o ciberterrorismo na Paraíba por meio de cenários prospectivos. Este objetivo foi alcançado com o desenvolvimento do método e a construção de três cenários possíveis. Com ator "governo" influenciando fortemente as ações das organizações estudadas, a descrição do "cenário provável" é a mais próxima da realidade dos participantes da pesquisa.

Os resultados demonstram que estas organizações têm consciência da relevância da segurança da informação para garantir a manutenção de seus processos e projetos, mas em suas respostas os participantes relatam que há falhas ou vulnerabilidades que podem ser exploradas.

Um ponto de alerta identificado foi que as organizações estudadas não possuem mecanismos específicos para tratar as vulnerabilidades relacionadas ao ciberterrorismo. Estão cientes do problema pois sofreram algum tipo de incidente nos últimos anos, contudo até a conclusão desta pesquisa não haviam apresentado ações de prevenção a este tipo de ataque, permanecendo vulneráveis.

REFERÊNCIAS

ALBAHAR, Marwan. Cyber Attacks and Terrorism: A Twenty-First Century Conundrum. **Sci Eng Ethics**, 2017.

AHMAD, Rabiah *et al*. Perception on Cyber Terrorism: A Focus Group Discussion Approach. **Journal of Information Security**, 3, p. 231-237, 2012.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC. Rede Nacional de Ensino e Pesquisa - RNP. **Cais em Resumo**: alertas, vulnerabilidades e incidentes de segurança, n.5, set. 2015. Disponível em: <https://www.rnp.br/sites/default/files/media/cais-resumo_maio-agosto-2015.pdf>. Acesso em: 13 fev. 2018.

_____. Ministério da Ciência, Tecnologia, Inovações e Comunicações - MCTIC. Rede Nacional de Ensino e Pesquisa - RNP. **Cais em Resumo**: alertas, vulnerabilidades e incidentes de segurança, n.6, 1º semestre de 2017. Disponível em: <https://www.rnp.br/sites/default/files/06_caisemresumo_ago_rb.pdf>. Acesso em: 13 fev. 2018.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL - CERT.br. **Estatísticas mantidas pelo CERT.br**. 2016. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>. Acesso em: 07 set. 2017.

GODET, Michel; DURANCE, Philippe. **A prospectiva estratégica para as empresas e os territórios**. UNESCO, 2011.

GODET, Michel. **From anticipation to action**: a handbook of strategic prospective. Paris: Unesco, 1994.

GORDON, Sarah; FORD, Richard. Cyberterrorism? **Computers & Security**, v. 21, n. 7, p. 636-647, 2002.

PWC. **A global state of information Security. 18.ed.** Disponível em: <http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html>. Acesso em: 20 Set. 2016.