UMA CULTURA DE SEGURANÇA CIBERNÉTICA GLOBAL E MULTINÍVEL

Glaucio da Rocha Silveira [1]
Argentino José Braga Bueno [2]

RESUMO

Este artigo pretende argumentar sobre uma cultura de segurança cibernética global e multinível. Para atingir esse objetivo, o estudo irá definir segurança cibernética em relação a um conceito mais amplo de segurança. Nesse sentido, é necessário analisar a evolução do conceito, principalmente a partir da Guerra Fria, e sua relação com a definição de segurança nos dias de hoje. Em seguida, com igual necessidade, o presente trabalho irá definir e identificar o objeto referente à segurança, a importância das ameaças cibernéticas e a necessidade de uma gestão de múltiplos níveis no que tange à segurança e às ameaças cibernéticas. Essa administração somente é possível e eficaz através do desenvolvimento de uma cultura de segurança composta de múltiplos níveis de segurança. O presente estudo ainda aborda a ideia de um quadro global de cooperação em múltiplos níveis, baseado em uma estratégia que visa o desenvolvimento de uma cultura de segurança cibernética global. Essa cultura deve ser implementada gradualmente, baseada na cooperação horizontal e vertical, começando com questões de segurança de baixa sensibilidade política. À luz da revisão bibliográfica, observa–se que o Brasil já está no caminho da implementação de uma cultura multinível, através da realização de acordos de cooperação com países amigos, apesar de se tratar de um tema bastante recente na área. Cabe salientar ainda que, apesar do esforço realizado pela APF, um estudo apresentado pelo Tribunal de Contas da União – TCU, através do acórdão 3.117/2014, demonstra a baixa adesão dos órgãos públicos no intuito de implementar a cultura de segurança.
Palavras-Chave: Segurança e Defesa Cibernética. Espaço Cibernético. Cultura de Segurança. Gestão da Segurança da Informação.

1 INTRODUÇÃO

Diversos historiadores consideram que o início do processo de globalização data do séc. XV e XVI, período em que ocorreram as grandes navegações e descobertas marítimas. No contexto do presente estudo, o conceito de globalização engloba diversas atividades, como as sociais, políticas e econômicas, passando pelas diversas fronteiras e regiões do mundo, de modo que acontecimentos e decisões ocorridos em qualquer ponto do globo podem possuir impactos e significados relevantes em outro(s) ponto(s) distintos.

Pode-se, então, dizer que a tecnologia é um dos principais fatores aceleradores da globalização. Dada essa aceleração, o tempo e o espaço têm diminuído. Nos dias atuais, o rápido aumento das interações humanas globais - com o uso de ferramentas como o Whatsapp,

[1]Engenheiro Eletricista com ênfase em Computação, MBA em Gestão de Tecnologia da Informação Executivo ênfase Petróleo e Gás Natural, pela Universidade Federal do Rio de Janeiro – UFRJ.
[2]Orientador. Professor do Centro Universitário do Sul de Minas/ UNIS-MG. E-mail: argentinojose@yahoo.com.br.

Facebook e outras redes sociais, transações financeiras, cooperação internacional e a crescente importância de atores não-estatais nos assuntos globais - é possível graças ao uso da tecnologia cibernética. Em suma, o espaço cibernético gerou um novo contexto de mundo, onde as fronteiras físicas deixam de ser um fator limitador e os seus atores são os mesmos da vida cotidiana. Fazendo com que, inclusive, fatos ocorridos em quilômetros de distância impactem diretamente em acontecimentos locais e vice-versa.

Então como abordar os problemas de segurança gerados pelas chamadas "ameaças cibernéticas"? O presente estudo argumentará sobre uma cultura de segurança cibernética global e multinível. Para atender ao objetivo proposto, este artigo abordará o conceito de segurança cibernética em relação ao conceito tradicional de segurança. Isso será feito através do estudo do conceito de segurança, principalmente após o período da Guerra Fria até os dias atuais. Em seguida, serão identificadas as principais ameaças cibernéticas e a importância de uma gestão de segurança em múltiplos níveis. E, por fim, será apresentada uma visão sobre a cultura de segurança da informação na Administração Pública Federal.

2 CONCEITOS BÁSICOS

2.1 Segurança X Segurança Cibernética

Para entender a importância da segurança na política global e nas relações internacionais, basta realizar uma análise de sua interferência na vida das pessoas diariamente. De modo tradicional, até a Guerra Fria, segurança abordava o conceito de ameaça entre Estados. A partir de então, novos conceitos de segurança foram adotados: segurança humana, segurança da sociedade, segurança ambiental, segurança coletiva e cooperativa. Evidentemente, surgiu a necessidade de enfrentamento de ameaças decorrentes de um contexto globalizado, como conflitos regionais, terrorismo, crime organizado etc.

De acordo com a teoria realista, segurança foi expressa através de quatro elementos chave: "estado, estratégia, ciência e o status quo ou estado atual". Esse conceito teve papel nitidamente relevante durante a Guerra Fria. A competição entre as duas maiores potências do sistema internacional, a corrida armamentista e o medo de uma guerra nuclear potencial foram algumas características que marcaram a Guerra Fria e a influência política para a tomada de decisões externas dos EUA, da União Soviética e seus aliados. (CARAYANNIS; CAMPBELL; EFTHMIOPOULOS, 2014).

Com o fim da bipolaridade, esse entendimento predominante sobre segurança passa a ser seriamente desafiado. O colapso da União Soviética deu fim à ideia de estratégia militar como o principal conceito de segurança, abrindo brechas para novas ameaças, iniciando-se, assim, o debate sobre as formas de abordar e conceituar segurança. Fatores como desmilitarização, expansão da democracia, evolução da tecnologia, das comunicações e, portanto, da globalização, ampliaram o campo de estudos sobre segurança. A partir disso, este estudo adota segurança como sendo associada à redução das ameaças aos valores estimados, especialmente aqueles que podem ameaçar a sobrevivência de um objeto referente particular em um futuro próximo.

Baseando-se na literatura sobre estudos de segurança, é possível definir quatro perguntas que ajudam a compreender a importância da segurança cibernética e a forma como uma cultura

de segurança multinível poderia ser formulada. Quais sejam: Qual é objeto referente de segurança? Qual é a ameaça à segurança? Quem é o responsável por fornecer segurança? Quais as melhores maneiras de fornecer segurança?

Durante a Guerra fria, pode-se afirmar que o objeto referente de segurança era o Estado, ou seja, foi o objeto mais ameaçado e, por isso, necessitou de defesa. Com o passar do tempo, a segurança do indivíduo e seu bem estar tornaram-se cada vez mais importantes. Assim, entende-se que a segurança do indivíduo está diretamente relacionada à Segurança Nacional e, portanto, deve ser priorizada. (CHOUCRI, 2012)

Para que uma cultura de segurança em vários níveis seja implementada, é necessária a observação de vários objetos de referência. No contexto de segurança cibernética, a preocupação deve estar voltada para o indivíduo e para a sociedade, nos níveis nacional/estadual, regional e/ou nível internacional. Todos esses níveis, muitas vezes interligados, constituem o objeto referência em questão. O espaço cibernético criou um "universo paralelo", em que esses níveis coexistem em todos os momentos e em todos os aspectos da vida social, política e econômica. Cabe salientar, entretanto, que o espaço cibernético não é um bem global, como o mar, pois partes dele estão sob controle soberano. Logo, em um mundo globalizado, o espaço cibernético torna-se objeto de referência multinível e, embora de nível único, precisa ser protegido em todos os seus subníveis.

2.2 Objeto Referente e Ameaça

A partir da definição do objeto referente de segurança cibernética, o próximo passo é identificar o que constitui uma ameaça. De acordo com o objeto referente (estados, indivíduos, grupos sociais), os valores estimados variam e, portanto, deve-se avaliar quais estão sendo ameaçados e por que ou quem. Também não se deve esquecer que a segurança está diretamente relacionada com o conceito de paz e segurança internacionais; portanto, algumas agendas de ameaças são mais importantes do que outras, em termos de seu significado político ou dependendo do significado de quem define a agenda. Por exemplo, a agenda de ameaça no painel da ONU sobre Ameaças, Desafios e Mudança é, provavelmente, mais importante que qualquer outra agenda na política internacional. No entanto, ameaças virtuais variam em natureza e não podem ser limitadas ao terrorismo cibernético, pois facilmente se identifica lutas sobre a arquitetura da internet e da gestão do espaço cibernético, conflitos em busca de vantagem política e ganho econômico (seja legal ou ilegal) e ameaças à segurança cibernética Nacional (CARAYANNIS; CAMPBELL; EFTHMIOPOULOS, 2014).

Nesse contexto, os vários tipos de ameaças cibernéticas poderiam afetar direta ou indiretamente aspectos da vida social, política e econômica, por meio da interrupção ou destruição de infraestruturas críticas, como por exemplo, de acordo com a CIA, o Brasil já sofreu pelo menos dois apagões de energia elétrica graças a ataques hacker. Um documento da Comissão Europeia, em 2005, afirmou claramente que infraestruturas críticas incluem os recursos físicos, serviços e instalações de Tecnologia da Informação, redes e ativos de infraestrutura cuja perturbação ou destruição teria um sério impacto sobre a saúde, segurança ou o bem estar econômico dos cidadãos ou para o funcionamento eficaz dos governos. Então, ameaças cibernéticas estão diretamente associadas à segurança humana, nacional, internacional

e, portanto, global, podendo facilmente ser convertidas em outro tipo de ameaça, como as de natureza econômica, alimentar, saúde, meio ambiente, demográficas, entre outras. Portanto, fica claro que a segurança cibernética é importante para todos, mesmo para aqueles que não possuem um computador pessoal.

2.3 Provedor e Políticas de Segurança

As duas últimas perguntas estão claramente interligadas, já que as políticas de fornecimento de segurança não são apenas relacionadas diretamente ao objeto referente e às ameaças de segurança, mas também ao provedor de segurança. Os responsáveis por prover a segurança podem variar em tamanho, influência e importância, especialmente no âmbito das relações internacionais. Nessa visão, o provedor de segurança pode ser qualquer um, desde o Estado a uma organização não governamental, ou mesmo indivíduos com certas capacidades e em determinadas situações. Dependendo da ameaça, podemos afirmar que alguns provedores serão mais capazes que outros. À medida que as agendas de ataque aumentam, existe a necessidade da atuação de diversos atores para lidar com as ameaças daí decorrentes. Tendo em vista que as ameaças de hoje são muitas e não seguem as linhas tradicionais, os responsáveis pela segurança, bem como as políticas e mecanismos de defesa, devem ser ajustados em conformidade. Além disso, o mundo cada vez mais globalizado e a interconexão do sistema internacional desafiam a soberania do Estado e transnacionalizam ameaças, tornando, assim, a adoção de políticas comuns necessárias.

É importante retratar que a adoção de políticas internacionais, por si só, não é uma solução para o problema, pois ameaças específicas que podem ser consideradas importantes para certos indivíduos, Estados ou atores diversos talvez não recebam a atenção desejada por parte de agentes de segurança exclusivamente internacionais. No caso de uma segurança multinível, o cenário passa a ser diferente uma vez que o provedor de segurança não se limita às políticas nacionais ou internacionais de gestão de segurança. Ao invés disso, seu objetivo seria integrar em uma estrutura comum e coletiva todos os níveis envolvidos, de forma a serem capazes de produzir políticas públicas, orientando globalmente sobre defesa e segurança cibernética (CLOUTH, 2004).

Pode-se, então, definir segurança cibernética como sendo a capacidade coletiva do indivíduo, não estatal, nacional e atores internacionais para proteger cada um desses níveis contra qualquer tipo de ameaças cibernéticas, através de uma estrutura de múltiplos níveis de cooperação, com o fim de proporcionar uma gestão global do espaço cibernético seguro e estável. Para atingir esse conceito, é necessário desenvolver uma cultura de segurança que corresponda adequadamente a este desafio.

Entende-se, portanto, que essa cultura deve ser ampla, capaz de transpor as diferentes culturas estratégicas nacionais, de modo a agrupar as diversas características comuns, criando uma cultura nova e coletiva.

3 GOVERNANÇA OU GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Face aos conceitos apresentados até o momento, surge uma nova inquietação, seria possível realizar governança e gestão, em caso da aplicação desta cultura global?

Lima-Marques e Marciano (2006) definem que a correta gestão ou governança da segurança da informação é atingida com o compromisso de todos os usuários quanto à aplicação das normas e procedimentos estabelecidos. Definem, ainda, que o termo "governança" tem sido usado para indicar as atividades de planejamento, implementação e avaliação das atividades voltadas à segurança, agrupando estas atividades conforme a seguinte disposição:

a) desenvolvimento de políticas, com os objetivos da segurança como fundamentos em torno dos quais elas são desenvolvidas;
b) papéis e autoridades, assegurando que cada responsabilidade seja claramente entendida por todos;
c) delineamento, desenvolvendo um modelo que consista em padrões, medidas, práticas e procedimentos;
d) implementação, em um tempo hábil e com capacidade de manutenção;
e) monitoramento, com o estabelecimento de medidas capazes de detectar e garantir correções às falhas de segurança, com a pronta identificação e atuação sobre falhas reais e suspeitas com plena aderência à política, aos padrões e às práticas aceitáveis;
f) vigilância, treinamento e educação relativos à proteção, operação e prática das medidas voltadas à segurança.

Em consonância com a definição acima apresentada, o framework COBIT, mantido pela ISACA *Information Systems Audit and Control Association* (Associação de Auditoria e Controle de Sistemas de Informação), é formado por um conjunto de boas práticas e recomendações de governança de Tecnologia da Informação mundialmente reconhecidas. Atualmente, está em sua quinta versão, contando com uma arquitetura formada por quatro domínios: planejar e organizar, adquirir e implementar, entregar e suportar, monitorar e avaliar. Essa organização funcional ainda conta com 34 processos e 210 pontos de controle.

Como esse tema é muito recente, apenas no final de 2014 foi lançada pelo ISACA uma série de certificações na área de segurança cibernética, incluindo dois cursos de treinamento de cibersegurança: Implementando o NIST (*National Institute of Standards and Tecnology*) *Cybersecurity Framework* usando COBIT 5 e COBIT 5 *Assessor for Security*.

4 CULTURA DE SEGURANÇA DA INFORMAÇÃO NA ADMINISTRAÇÃO PÚBLICA FEDERAL

O Brasil ainda se encontra em estágio inicial no que tange à implementação de uma cultura de segurança cibernética, apesar dos esforços apresentados pelo Governo Federal que, desde os anos 2000, demonstra sua preocupação com o tema. Em 2015, foi publicada a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética para os anos de 2015 – 2018. Nessa esteira, é importante citar algumas das ações constantes na Estratégia e já realizadas pelo Governo Federal, especialmente a partir dos anos 2000, com o fito de promover o desenvolvimento de um modelo cultural e de gestão de segurança da informação no País.[1]

[1] O anexo poderá ser acessado via link: http://bit.ly/2pFivyk.

5 CONSIDERAÇÕES FINAIS

Acredita-se, então, que o passo dado pelo ISACA pode ser considerado o primeiro passo em nível de desenvolvimento de uma cultura de cooperação e segurança em múltiplos níveis. Essa cultura seria informada por todos os níveis através de uma abordagem *top-down/bottom-up* sem a imposição de regras, regulamentos ou políticas de um nível em outra. Em um nível subnacional, os atores não estatais, como bancos, empresas de transporte, comunicação etc. teriam mais facilidade em obter colaboração do que os próprios Governos. Portanto, existe a necessidade da criação de uma rede global, que iria, principalmente, lidar com preocupações de segurança cibernética comercial de entidades privadas.

Tais preocupações podem ser interrupções cibernéticas, bem como dados ou roubo de inteligência por indivíduos, ou outras entidades privadas. Muitos Estados já criaram sua própria ciberdefesa, não só para fins militares, mas também para a segurança da sua administração e infraestrutura. No entanto, esse conhecimento, tanto quanto possível, deve ser compartilhado com outros Estados, em um âmbito de cooperação global. As organizações regionais podem desempenhar um papel fundamental para esse fim. Entidades como a OTAN, a União Europeia, a Associação de Nações do Sudeste Asiático e o Mercosul, entre outras, podem facilitar o diálogo internacional sobre segurança cibernética como um próximo passo. Compreensivelmente, algumas dessas instituições estão mais focadas na cooperação comercial e econômica; o foco em segurança cibernética seria uma possibilidade de maior integração.

Entretanto, a nível Nacional, os atores não estatais devem ser, em coordenação tanto com o governo quanto com a instituição regional relevante, a chave para uma integração global das diferentes entidades e preocupações sobre o tema, através do diálogo inter-regional / organizacional. Esse seria o último passo para a conclusão do sistema de múltiplos níveis e globalmente orientado à cooperação.

Em suma, horizontalmente, se os atores não estatais com base em diferentes estados devem cooperar entre eles, os estados também devem cooperar a nível governamental (bilateral ou multilateral), os Estados devem participar em instituições internacionais de sua região, e as instituições regionais devem participar na coordenação inter-regional. Verticalmente, todos os níveis devem manter uma linha de comunicação eficaz e coordenação entre eles.

A cooperação deve começar a partir da vida comercial, todos os dias, e, nomeadamente, não estatal, de modo a proceder gradualmente para questões nacionais, governamentais e militares. Desse modo, o desenvolvimento de uma cultura de segurança cibernética em múltiplos níveis de segurança global seria possível e com maior potencial não só para a segurança cibernética, mas para a paz internacional.

Por fim, apesar do Acórdão 3.117/2014 – TCU apontar para uma baixa adesão da APF, no sentido de implementar uma Cultura de Segurança Cibernética Nacional, incluindo a sua gestão, pode-se afirmar que o Brasil adere ao princípio estudado, principalmente através da realização de

acordos de cooperação, para troca e proteção mútua de informações com diversos países, como Suécia, Israel, Itália, Rússia e Espanha.

5.1 Trabalhos Futuros

Como expectativa natural de evolução do presente artigo, um estudo sobre o certificado da ISACA, implementando o NIST (*National Institute of Standards and Tecnology*) *Cybersecurity Framework*, usando COBIT 5 e seus possíveis impactos em caso de adoção nas Autarquias Federais, especialmente no que tange à cultura de segurança da informação.

A GLOBAL AND MULTILEVEL CYBERSECURITY CULTURE

ABSTRACT

This article intends to argue for a comprehensive and multi-level cybersecurity culture. To achieve this objective the study will define cybersecurity, in relation to a broader concept of security. In this sense it is necessary to analyze the evolution of the concept, especially since the Cold War, and its relationship to the concept of security today. Then define and identify the referent object of security, the importance of cyber threats and the need for multiple levels of management with respect to security and cyber threats. This administration is only possible and effective, through the development of a safety culture composed of multiple levels of security. This study also discusses the idea of a global framework for cooperation on multiple levels based on a strategy for the development of a global culture of cybersecurity. This culture should be implemented gradually, based on horizontal and vertical cooperation, starting with security issues of low political sensitivity. In light of the literature review notes - that Brazil is already on the way of implementing a multilevel culture through the implementation of cooperation agreements with friendly countries, although it is a fairly recent topic in the area. It should be noted also that despite the efforts made by the APF, a study presented by the Federal Audit Court - TCU, by judgment 3117/2014 demonstrates the low compliance of public bodies in order to implement safety culture.

Keywords: Security and Defense Cybernetics. Cyberspace. Safety Culture. Information Security Management.

REFERÊNCIAS

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Estratégia de segurança da informação e comunicações e de segurança cibernética da administração pública federal 2015-2018 : versão 1.0** / Gabinete de Segurança Institucional, Secretaria-Executiva, Departamento de Segurança da Informação e Comunicações. Brasília : Brasil, 2015.

CAMPOS, L., CANAVES, S.. **Introdução à Globalização**. Disponível em http://www.rdpc.uevora.pt/bitstream/10174/2468/1/Introdu%C3%A7%C3%A3o%20%C3%A0%20Globaliza%C3%A7%C3%A3o.pdf . Acesso em: 31 maio 2016.

CARAYANNIS, Elias G; CAMPBELL, David F.J.; EFTHYMIOPOULOS, Marios Panagiotis. **Cyber-Development, Cyber-Democracy and Cyber-Defense, Chalenges, Opportunities and Implications for Theory, Policy and Practice**. Springer, 2014.

CARDOSO, Carlos Frederico Varela. **Cultura de Segurança e Cidadania.** FCSH. Pós Graduação em Estudos Estratégicos e de Segurança, PT, 2014.

CHOUCRI, N. **Cyberpolitics in International Relations**. MIT Press, 2012.

CLOUTH, Cris. Quid Pro Quo: The Challenges of International Strategic Intelligence Cooperation. **International Journal of Intelligence and CounterIntelligence**, v. 17, p. 601 – 613, 2004.

MANDARINO JÚNIOR, Raphael. **Um Estudo sobre a Segurança e Defesa do Espaço Cibernético Brasileiro.** Monografia Especialização. UNB. Instituto de Ciências Exatas, Departamento de Ciência da Computação. Brasília, DF, 2009.

MARCIANO, João Luis; LIMA-MARQUES, Mamede. O Enfoque Social da Segurança da Informação. **Ci. Inf., Brasília**, v. 35, n. 3, p. 89-98, set./dez. 2006.

MARTINS, Henrique dos Santos, NUNES, Paulo, SILVA, Rui. **Framework de Gestão de Segurança da Informação para Organizações Militares Orientada pelos Principais Vetores de Ataque**, 2016. Disponível em: http://docplayer.com.br/8009979-Framework-de-gestao-de-seguranca-da-informacao-para-organizacoes-militares-orientada-pelos-principais-vetores-de-ataque-resumo.html. Acesso em: 31 maio 2016.

SOUZA, Carlos Vendet. **Estudo sobre a Implementação de Equipes de Tratamento e Resposta de Incidentes de Rede na Administração Pública Federal. Monografia Especialização.** UNB. Instituto de Ciências Exatas, Departamento de Ciência da Computação. Brasília, DF, 2011.