CIBERSEGURANÇA E PARCERIAS PÚBLICO-PRIVADAS[1]

Evandro Gomes Laranjeira

Resumo: Ataques cibernéticos mostram-se cada vez mais como a maior ameaça a ser enfrentada por Estados e empresas. Tanto o setor privado quanto o público veem-se como vítimas de brechas de segurança e vazamentos de dados sensíveis. Os ataques podem ser provenientes de qualquer local, de dentro ou fora do território nacional, motivados por outros agentes estatais ou privados.

Em geral, entende-se que os setores público e privado precisam colaborar para enfrentar os desafios de segurança cibernética da nação. Embora as parcerias público-privadas tenham sido frequentemente estimuladas e, em casos pontuais desenvolvidas, esta relação por vezes se mostra problemática. Existe uma ambiguidade persistente em relação às expectativas e deveres, resultando em uma parceria sem linhas claras de responsabilidade para ambos os lados.

Os obstáculos jurídicos, estratégicos e pragmáticos dificultam frequentemente a cooperação efetiva entre o setor público e o setor privado, que são agravados pelos riscos regulamentares e de responsabilidade civil. Estes fatores são complicados ainda mais por questões transfronteiriças, incluindo leis e perspectivas inconsistentes sobre, em particular, normas e restrições de privacidade, transferência de dados e interesses políticos divergentes na luta contra as ameaças cibernéticas.

Desta forma, este trabalho almeja avaliar o cenário atual e as possíveis atribuições de papéis para ambos os atores (estatais e privados) em parcerias para melhoria da segurança cibernética.

Palavras-chave: cibersegurança, parcerias público-privadas, segurança da informação

[1] Artigo apresentado como Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista Gestão de Segurança da Informação.

1 INTRODUÇÃO

O conceito de Segurança da Informação na sociedade de hoje evoluiu de uma abordagem local para global. Nos últimos anos tem-se notado que alguns dos principais serviços de um país que pertenciam ao Estado, neste momento estão compartilhados entre Estado e iniciativa privada, tanto nacionais, como estrangeiros.

Cavelty e Brunner (2009) em estudo sobre as implicações da era da informação para a política internacional, reforçam que "o desenvolvimento tecnológico aumenta duas tendências que diminuem a importância do Estado, que têm implicações para a segurança: aumento da internacionalização e crescente privatização".

Segundo Germano (2014), o termo "Segurança cibernética" ou “Cibersegurança” é quase tão amplo e indistinto como a própria "segurança" e há uma série de razões para isso. Em primeiro lugar, pode-se citar as implicações da Internet nos diversos sistemas críticos e práticas em vários níveis. Outros pontos a serem destacados são transações comerciais/bancárias, ameaças militares, proteção da propriedade intelectual, privacidade pessoal, segurança de infraestruturas críticas etc. Estas áreas variam muito e são unidas apenas pela tecnologia com a qual elas se envolvem.

Os ataques às infraestruturas críticas continuam sendo um dos temas dominantes nos debates sobre a segurança cibernética em todo o mundo. Ao longo da última década, esse tipo de ataque não só surgiu como uma ameaça isolada, mas também no contexto de ataques organizados, que atentam contra a segurança nacional, como demonstrado na Estónia em 2007, na Geórgia em 2008 e, claramente, no episódio Stuxnet de 2010.

Deve-se notar que neste cenário a parceria público-privada torna-se uma necessidade na cibersegurança nacional. A Intel Security em conjunto com o Aspen Institute (2015), realizaram uma pesquisa com 600 executivos de tecnologia na França, Alemanha, Reino Unido e Estados Unidos para identificar os desafios para proteção em infraestruturas críticas. Grande parte (86%) dos respondentes apontaram para uma necessidade de parcerias público-privadas de compartilhamento de inteligência para estarem em dia com as ameaças à segurança ciberné-tica cada vez mais frequentes.

Os governos têm relações diversas com provedores de serviços de Internet, empresas multinacionais de informação (Google, Facebook, etc.), empresas privadas de cibersegurança, promotores de direitos humanos e civis, agências policiais e sociedade civil. No entanto, a parceria público-privada é muito limitada, ignorando sua

complexidade, onde setores críticos da indústria de energia e bancos para transporte e atendimento de saúde respondem a diferentes agências governamentais ou reguladores. Portanto, é imperativo que qualquer gestor de cibersegurança corporativa sustente fortes relações de trabalho com partes governamentais interessadas e apropriadas.

O primeiro grande obstáculo à cooperação envolve questões de confiança, benefício, risco e controle. Em alguns casos a resistência reside em os líderes da organização privada terem a certeza de que o governo não causará interferências indevidas em suas as operações. Isto, muitas vezes, gera a percepção de que a empresa é capaz de melhor e mais eficazmente resolver o problema por conta própria, sem a intervenção do governo.

No âmbito estatal, notamos que a falta de compreensão neste tipo de ameaça, faz com que a abordagem, bem como a implementação de soluções torne-se equivocada, como observado no Brasil, na criação do Centro de Defesa Cibernética do Exército Brasileiro (o CDCiber), encarregado da defesa cibernética do país. Curiosamente, esta resposta possui foco limitado (militarização) em apenas algumas dimensões destas ameaças – em especial as transnacionais (Muggah, Glenn e Diniz, 2014)

2 DISCUSSÃO

I. IMPORTÂNCIA

O Brasil desenvolveu uma infraestrutura de cibersegurança que tende em maior grau às prioridades militarizadas e securitizadas (governo), visando em especial alguns tipos específicos de ameaças cibernéticas e não contemplando outras. (Artigo 19, 2017)

Resolver este problema é de importância crítica porque, devido às características inerentes à Internet e, ao contrário de muitas infraestruturas tradicionais, será impossível para o governo criar um sistema sustentável de cibersegurança sem a participação ativa, voluntária e contínua do sector privado.

II. PARCERIAS PÚBLICO-PRIVADAS

Para analisar esta questão crítica é necessária a clareza da definição, onde numa verdadeira parceria, as entidades com poder sobre a relação e mesmo que tenham algumas metas e objetivos diferentes, concordam em comprometer os seus interesses e

desenvolver conjuntamente um plano de ação para obter ganho mútuo para os objetivos uns dos outros, bem como objetivos mútuos.

No caso dos setores público e privado trabalhando em conjunto, o papel do governo é servir o interesse público mais amplo. A meta legalmente obrigatória da indústria é geralmente servir o interesse do acionista.

Assim, quando o governo exige a adequação da indústria em uma nova regulamentação, não obstante o esforço colaborativo, não pode ser verdadeiramente considerada uma "parceria", uma vez que o governo tem poder sobre a entidade regulamentada para definir o plano de ação e a entrada da indústria é principalmente de servir os objetivos do governo (ou do público em geral).

Da mesma forma, quando a indústria ajuda voluntariamente o governo em busca de um objetivo governamental (apoio a serviços essenciais ou situações de emergência, por ex.), apesar do esforço cooperativo e o inquestionável objetivo do Estado, esta não é uma parceria público-privada, uma vez que os interesses dos acionistas não estão sendo atendidos. Os planos de ação para esses esforços são, adequadamente, dirigidos pelo governo e os objetivos são servir ao interesse público, não ao interesse privado, eles tendem a ser difíceis de sustentar além da situação emergencial e especialmente difíceis de sustentar a longo prazo.

III. FUNÇÕES E RESPONSABILIDADES

As parcerias público-privadas atuais em seu modelo atual têm papéis mal definidos e responsabilidades para a indústria e os parceiros governamentais. Certamente a especificação de papéis e responsabilidades pode ser difícil e a falta de fazê-lo quase certamente levará à confusão e ineficiência que pode e deve ser evitada.

Praticamente todas as relações de negócios, incluindo aquelas entre o governo e a indústria privada, especificam claramente os papéis e responsabilidades dos parceiros. No que diz respeito à segurança cibernética, propomos que os papéis e responsabilidades devem ser baseados no seguinte modelo.

Papel do governo

1. garantir a infraestrutura governamental;
2. servir como modelo para a indústria;
3. fornecer informações da indústria em um formato oportuno e em tempo útil;
4. assegurar infraestrutura privada operando sob acordos fornecidos pelo governo (por exemplo, serviços públicos) são seguras dentro dos limites dos requisitos de interesse público;
5. incentivar as empresas que operam em ambientes não regulados a investir em segurança no interesse público para além do que a entidade privada fará para servir os seus interesses privados;
6. proporcionar desenvolvimento e avaliação de pesquisas a tecnologias e práticas de segurança cibernética para as quais não exista um interesse direto do setor privado;
7. educar o público sobre segurança cibernética.

Funções da Indústria

1. inovar, desenvolver e lançar no mercado tecnologias que possam tornar uma infraestrutura segura;
2. desenvolver normas e práticas para enfrentar a ameaça cibernética em constante evolução;
3. compartilhar informações com o governo de acordo com o interesse público sem violar suas responsabilidades corporativas;
4. trabalhar com o governo para desenvolver mecanismos e melhorar a segurança cibernética em geral;
5. implementar boas tecnologias e práticas de segurança consistentes com suas responsabilidades.

IV. PRINCÍPIOS

Na administração da cibersegurança nacional, o Gabinete de Segurança Institucional (GSI) é o órgão governamental chave que trata de todos os aspectos civis de cibersegurança. Dentre outros órgãos envolvidos na formulação de políticas de cibersegurança, podemos destacar o Departamento de Segurança da informação e

Comunicações (DSIC), Secretaria de Assuntos Estratégicos (SAE), Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN). O conjunto DSIC, SAE e CREDEN são os protagonistas chave na formulação dos debates sobre a cibersegurança no país. (Artigo 19, 2017)

Esta estrutura de cibersegurança atribui competências a seus principais agentes, onde a Polícia Federal está encarregada de combater a criminalidade comum (inclusive as investigações), ao passo que o Exército deve empreender a defesa do ciberespaço nacional contra a ciberguerra e o ciberterrorismo

No entanto, essas políticas acabam por serem ideologicamente baseadas e, seus esforços isolados, não percebem que o objetivo não é necessariamente o que é "correto", mas o que vai funcionar dentro da ótica governamental. Os recursos nessas parcerias têm sido frequentemente controlados pelo governo e inadequados ou condicionados ao cumprimento de critérios especificados pelo governo (ou por vezes não especificados), levando ao controle funcional do parceiro governamental sobre o programa, prejudicando assim o compromisso da parceria e do setor privado.

Para reforçar o estado das parcerias para a segurança cibernética, existem 5 princípios centrais a serem seguidos:

A. O pragmatismo, e não a ideologia, deve reger a parceria;
B. deve haver uma apreciação mais completa de ambas os objetivos do parceiro;
C. Planos de Ação devem ser desenvolvidos conjuntamente;
D. os mecanismos existentes do setor privado deveriam ser mais utilizados;
E. A avaliação constante deve ser parte integrante no escopo das parcerias.

Esses princípios pragmáticos muitas vezes não estiveram presentes nas parcerias público-privadas existentes. Por diversas vezes as organizações foram criadas sem missões claras, para além da "coordenação" e, em seguida, os projetos são adaptados às estruturas existentes. (Muggah, Glenn e Diniz, 2014).

A - O pragmatismo, e não a ideologia, deve reger a parceria

O ponto essencial é que, à medida que o governo procura estabelecer um acordo de parceria com a indústria, precisa de se concentrar em não somente regulamentar o

funcionamento do mercado ou punir os maus atores, mas avaliar pragmaticamente que tipo de instrumentos disponíveis e quais são mais propícios a criar um ambiente sustentável. Desta forma, é possível evitar as distorções por interesses corporativos. (INSA, 2009)

A Internet é diferente de qualquer outra infraestrutura. Exige unicamente uma parceria público-privada criativa baseada nos pontos fortes dos princípios do mercado e do envolvimento do governo.

As parcerias público-privadas destinadas a resolver a questão da cibersegurança, devem:

- ter objetivos claros, razoáveis e mensuráveis;
- possuir recursos identificáveis adequados à tarefa para a qual a parceria foi concebida;
- ser cooperativo na natureza, sem detalhes punitivos caracterizados por modelos reguladores, de modo que a confiança e as medidas proativa positivas sejam tomadas por ambos as partes;
- possuir uma estrutura de liderança conjunta reconhecida em que ambos os parceiros acreditam ter investimento e controlo equivalentes sobre o funcionamento da parceria;
- criar planos de ação em conjunto, na qual ambos os parceiros desenvolvem as metas e objetivos do projeto de parceria a ser realizado.

B - Deve haver uma apreciação mais completa de ambos objetivos do parceiro

O objetivo maior da segurança cibernética para o governo é a defesa comum. Enquanto indivíduos e empresas se beneficiam de uma forte defesa nacional, o interesse nacional não é, e não deveria ser, o objetivo para os interesses privados.

Para o setor privado, o valor para investimentos em segurança cibernética é justificado por seus planos de negócios individualizados. As empresas podem e devem fazer investimentos em segurança cibernética alinhados com seu interesse privado, sendo que ao longo dos últimos anos, foram feitos investimentos substanciais para melhorar estas necessidades individuais de segurança no nível organizacional.

No entanto, cabe ao setor público assegurar a "defesa comum", que incluiria suprir as lacunas em áreas de segurança que não são justificadas por investimentos corporativos individuais. Ao cumprir esta responsabilidade pública, o governo tem uma série de ferramentas à sua disposição, bem como um ambiente favorável ao mercado.

Isso não significa que o governo deve analisar os planos de negócios individuais de cada entidade, mas sim que deve manter as empresas sensíveis e aos benefícios de interesse público.

C. Os planos de ação devem ser desenvolvidos conjuntamente.

Mesmo que a indústria tenha os maiores recursos e responsabilidades para lidar com a cibersegurança, o governo ainda se vê como o "parceiro principal" em seu relacionamento. Isso significa que, muitas vezes, quando as atuais parcerias público-privadas se envolvem em projetos, elas são tipicamente iniciadas pelos parceiros governamentais para tratar dos interesses do governo. Algumas das organizações privadas tentarão auxiliar o governo nesses projetos, mas a eficácia dos projetos é, às vezes, comprometida desde o início devido ao papel de "parceiro sênior" do governo.

Os planos de ação, a medida em que são desenvolvidos, são frequentemente elaborados pelos parceiros governamentais e depois fornecidos à indústria ostensivamente para comentários, mas apenas depois de os parceiros governamentais já terem se comprometido com o público em geral, o que fatalmente demonstra a pouca importância e confiança dada aos atores privados. (Germano, 2016)

Assim, os projetos caminham para metas que não foram desenvolvidas em parceria, o que leva a um comprometimento pouco entusiasmado com os setores privados, desperdício de tempo e esforço e produtos ou resultados que não são tão úteis quanto deveriam ser

Em vez de o governo aproximar-se de seus parceiros da indústria com uma estrutura organizacional pré-determinada, metas predefinidas e planos de governo, deve-se abordar a indústria com uma "página em branco" e trabalhar no desenvolvimento de planos de ação em verdadeira parceria.

4. Os mecanismos existentes do setor privado deveriam ser mais utilizados

O governo estabeleceu o caminho para as parcerias unilaterais, escolhendo estabelecer suas próprias entidades ou entidades que possuam algum vínculo direto com o governo (instituições de pesquisa estatais), invés de confiar na expertise do setor privado já existente e entidades que existiam. Isso deixou o setor privado sem escolha prática, mas para trabalhar através das organizações dominadas pelo governo.

Finalmente, conforme descrito acima, as atividades são dominadas pela agenda do governo, que os representantes da indústria lutam valentemente para ganhar paridade e verdadeira parceria com um sucesso limitado.

Ao invés de criar um universo paralelo de organizações do setor privado com o qual se associar, competindo assim com as associações da indústria, o governo poderia alavancar mais eficientemente as organizações existentes que a indústria estabeleceu um compromisso firme e reconhece como os representantes da indústria apropriada.

Essas organizações já têm um alcance muito maior dentro do setor privado do que as organizações patrocinadas pelo governo. Eles têm um reservatório de confiança, no tato pessoal profissional, recursos e uma história de compromisso de trabalhar em cooperação com o governo.

O problema para o governo de basear o seu relacionamento de cooperação com o setor privado usando seus representantes designados e não através de organizações patrocinadas por si mesmo, é que teria que desistir de algum de seu controle de "sócio principal".

O governo precisa decidir se a extensão de seu controle sobre os conselhos de coordenação do setor é mais valiosa do que o alcance expandido e o compromisso de resolver o problema de segurança cibernética que as organizações intactas forneceriam.

E. A avaliação deve ser parte integrante no escopo das parcerias

Conforme exposto acima, metas e objetivos mensuráveis e claros devem ser parte inerente do programa de parceria. Os objetivos para a parceria e os projetos desenvolvidos no âmbito desta devem ser sistematicamente avaliados regularmente.

Os recursos de avaliação devem ser incluídos em todos os programas empreendidos e a disponibilização de recursos adicionais para a continuação deve depender dos resultados da avaliação.

3 CONCLUSÕES

Este artigo mostra que as parcerias público-privadas são partes essenciais a segurança interna como um todo e, não apenas suas áreas de interesse. Tanto os atores públicos, quanto os privados enfrentam hoje riscos constantes, em alguns casos, imprevisíveis e inaceitáveis. Os adversários inovam em um ritmo acelerado e para deter seu progresso é necessária uma cooperação muito mais estreita entre o governo e o setor privado. Esta simbiose é um mecanismo crítico para negócios, governo e comunicação pessoal e deve ser preservado.

Do ponto de vista teórico, as parcerias público-privadas também levantam questões importantes. A compreensão de cibersegurança está cada vez mais ligada a conceitos, e não a ideologias. Flexibilidade, adaptabilidade e resiliência são necessárias na formulação programas e políticas de segurança em todos os níveis do governo. Incorporar esses conceitos nos planos e operações das agências ajuda a produzir resultados favoráveis.

Mas as parcerias público-privadas alinham-se suficientemente com esses conceitos, pois representam uma maneira "flexível" para expandir as capacidades do governo e, quando bem planejadas e implementadas não aumentam a dependência governamental do setor privado, reduzindo a flexibilidade organizacional.

Governo e cooperação empresarial podem fornecer vantagens únicas na contratação, utilização de recursos, especialização e inovação tecnológica. Essas parcerias também têm implicações significativas para as práticas de gestão, desafios legais e éticos, transparência, construção da participação do setor privado, política, orçamentação e planejamento de longo prazo.

Seja qual for a abordagem adotada, é crucial que alguém tome a iniciativa na resolução do problema e comece a abordá-lo de uma forma sistemática, através de uma

parceria de todas as partes interessadas. Estudos futuros precisarão examinar outras questões críticas que se tornem relevantes à medida que as parcerias público-privadas se intensificarem.

Um exemplo atual de sua importância refere-se aos efeitos causados pelos recentes ataques do ransomware Wannacry, onde o compartilhamento de informações para o alerta antecipado entre órgãos governamentais e empresas, poderia ter minimizado os danos aos dados e prejuízos financeiros.

REFERÊNCIAS

ASPEN INSTITUTE, INTEL SECURITY. *Critical Infrastructure Readiness Report Holding the Line Against Cyberthreats*. Disponível em http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf. Acesso em: 05 Nov. 2016.

ANDRESS, JASON.; WINTERFELD, STEVE. *Cyberwarfare – Techniques, Tactics and Tools for Security Practioners*, Syngress Press, EUA, 2ª ed., 324p., 2013.

CAVELTY MYRIAM D. SUTER, MANUEL. *Public–private partnerships are no silver bullet: an expanded governance model for critical infrastructure protection*, International Journal of Critical Infrastructure Protection, 181p., 2009.

DINIZ, G.; MUGGAH, R.; GLENNY, M. *Securitização da Cibersegurança no Brasil*. [s.l:s.n.]. v. 15

ETZIONI, AMITAI. *Cybersecurity in the private sector, Issues in Science and Technology*. Disponível em http://issues.org/28-1/etzioni-2/, Acesso em: 28 Out 2016.

GERMANO, JUDITH H. *Cybersecurity Partnerships: A New Era of Public-Private*. Disponível em http://www.lawandsecurity.org/wp-content/uploads/2016/08/Cybersecurity.Partnerships-1.pdf, Acesso em: 05 Nov. 2016.

INTELLIGENCE AND SECURITY ANALISYS, INSA. *Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models*, 2009.

VACCA, JOHN R. *Cyber Security and IT Infraestructure Protection*, Syngress Press, EUA, 1ª ed, 380p., 2014.