Repensando a guerra cibernética

Por Chris Archer/IDGA

Monitorar as ameaças cibernéticas é muito difícil, já que elas mudam de maneira abrupta e com muita frequência. Nesta entrevista, Chris Archer, do IDGA, explora o cenário atual e futuro da guerra cibernética com Scott Borg, diretor executivo do Cyber Consequences Unit, instituto de pesquisa norte-americano que avalia as consequências estratégicas e econômicas de possíveis ataques cibernéticos. Chris Archer pergunta como a guerra cibernética afetará a defesa no futuro e o que está sendo feito para garantir que os militares e o governo continuem se antecipando às ameaças. Scott Borg também revela os objetivos e as prioridades atuais do Cyber Consequences Unit.

Scott, em sua opinião, como a guerra cibernética afetará a defesa no futuro?

A guerra cibernética nos fará repensar cada aspecto da defesa. Nossos armamentos e sistemas de defesa atuais ainda serão necessários, mas o modo como os usaremos será muito diferente. Um grande ataque cibernético poderia driblar completamente nossas forças militares. Não demandaria aviões, mísseis, navios ou tropas. O ataque poderia aparecer de repente dentro do equipamento computadorizado de nossas indústrias mais importantes. Poderia ser impossível determinar de imediato, ou com toda a certeza, a identidade do país ou organização que foi responsável pelo ataque. O ataque cibernético poderia causar quase todo tipo de dano passível de ser produzido por operadores humanos de equipamentos computadorizados. De fato, um ataque cibernético poderia

causar muitos tipos de dano que os operadores humanos de equipamentos industriais só conseguiriam reprogramando seus controles.

Um ataque cibernético significativo poderia destruir ou sabotar fisicamente estações de geração de energia elétrica, refinarias, oleodutos, sistemas bancários, sistemas de controle ferroviário, centros de controle aéreo, usinas químicas, equipamentos de hospital e instalações de água e saneamento. Milhares de pessoas poderiam morrer imediatamente em decorrência de explosões, vazamentos de substâncias químicas tóxicas, acidentes de avião ou de trem e tratamentos médicos errados. Centenas de milhares poderiam ser levadas à morte com o passar dos meses em consequência de fome, doenças, falta de aquecimento ou refrigeração, e a escassez e o colapso social vivenciados quando um grande número de pessoas se vê impossibilitado de suprir suas necessidades vitais. O total de danos econômicos e fatalidades poderia ser superior ao de qualquer outro tipo de ataque, com a exceção do nuclear.

Nossa estratégia de defesa atual – o governo protegendo nossas fronteiras, pronto para aniquilar forças militares ou países adversários, e as indústrias domésticas ignorando totalmente as questões de defesa – claramente já não será adequada em um mundo em que esse tipo de ataque é possível. Toda a relação entre nossos militares e nossa sociedade precisará ser redefinida.

Você afirmou que o termo "ciberespaço" pode levar a confusões perigosas. Poderia explicar por quê?

A guerra cibernética tende a transformar por completo todos os tipos de operação militar, assim como a guerra mecanizada transformou todas as operações militares há cem anos. Declarar que o "ciberespaço" é um âmbito de combate, análogo à terra, ao mar e ao ar, é equivocado. Todo tipo de sistema de armamento e força militar que usa a microeletrônica, seja o exército, a marinha ou a força aérea, está hoje operando no "ciberespaço". Não há um âmbito separado de guerra cibernética. Imagine se os estrategistas militares do começo do século XX houvessem declarado um novo âmbito de combate chamado "espaço mecanizado", e destinado metralhadoras, aviões, tanques, caminhões e

todo tipo de novo dispositivo mecânico a uma "força mecanizada" separada. Isso seria análogo ao que nossos estrategistas militares estão fazendo atualmente quando falam de "ciberespaço" e começam a desenvolver uma "ciberforça" correspondente. Hoje, toda força militar é dependente da defesa cibernética, e toda força militar precisa ter um componente de força cibernética.

O próprio termo "ciberespaço" também leva a erros táticos e estratégicos, porque insinua que os conflitos cibernéticos ocorrerão em algo análogo a um espaço físico. Isso pode levar os líderes militares e estrategistas de defesa a pensar que o "ciberespaço" é algo com territórios e fronteiras; que há posições no ciberespaço que podem ser ocupadas; que, no ciberespaço, algumas coisas estão muito distantes e outras estão próximas; que atingir coisas "distantes" no ciberespaço leva mais tempo que atingir coisas que estão ao alcance da mão; que atacar mais localidades no ciberespaço requer mais combatentes; e assim por diante. Esse tipo de muitas vezes influencia decisões sobre a guerra cibernética, mesmo quando não estão declarados de maneira explícita. Esse tipo de pensamento é perigoso.

Por que é um desafio tão grande monitorar as ameaças cibernéticas?

O maior problema é que as ameaças cibernéticas mudam de maneira abrupta e com muita frequência. Prever a ocorrência de um ataque cibernético com base em outro que já aconteceu é de pouca utilidade, porque as ameaças com as quais estamos mais preocupados em um dado momento são diferentes daquelas que nos preocuparam dois ou três anos antes ou que nos preocuparão dois ou três anos depois. Lembra quando o grande receio era a propagação de vírus que obstruiriam sistemas ou apagariam os dados que não tivessem cópia de segurança? Ou, um pouco mais tarde, quando a grande preocupação era um ataque distribuído de negação de serviço (DDoS) a websites abertos ao público? Ou quando a grande ameaça eram as botnets, obstruindo a internet com spams? Ou alguma das outras ameaças cibernéticas que apareceram e praticamente desapareceram? Esta é uma área que está mudando a um ritmo alucinante.

A propósito, esse é o motivo pelo qual padrões de segurança determinados pelo governo geralmente não são uma boa ideia. Quando os padrões de segurança cibernética houverem sido definidos e estiverem entrando em vigor, eles não só estarão obsoletos, como muitas vezes serão um impedimento à implementação de medidas de segurança mais necessárias. Exigir que um software seja certificado causa problemas similares. Devido ao tempo requerido para passar pelos procedimentos de certificação, um software certificado quase sempre terá mais falhas de segurança que um software mais recente, não certificado. O governo não tem como garantir um bom nível de segurança cibernética; no máximo, consegue garantir um nível inadequado.

Conte-nos sobre os objetivos passados e atuais do Cyber Consequence Unit dos Estados Unidos (US-CCU). As prioridades e o foco da organização mudaram? O que o US-CCU está fazendo hoje?

O US-CCU é um instituto de pesquisa sem fins lucrativos que foi instaurado por solicitação do Gabinete do Setor Privado do Departamento de Segurança Interna dos Estados Unidos, logo que o departamento foi criado. Sua missão original era determinar quanto dano poderia efetivamente ser causado por vários tipos de ataque cibernético a indústrias de infraestrutura cruciais. A ideia era ter uma organização fora do governo que pudesse ter acesso a informações confidenciais das corporações, e proteger não só essas informações, como a própria identidade das corporações que as forneceram. Eu fui recrutado, porque sabia como quantificar, em termos econômicos, muitos tipos de dano que outras pessoas consideravam demasiado complicados ou intangíveis de quantificar.

O US-CCU foi muito bem-sucedido em sua missão original. Uma das coisas que descobrimos foi que muitos ataques cibernéticos seriam, na verdade, muito menos destrutivos do que se imaginava. Isso porque nossas principais indústrias são, em vários aspectos, muito engenhosas e resilientes. Também descobrimos que muitos ataques cibernéticos eram bem mais difíceis de se realizar do que se supunha. Nossa grande preocupação, tanto na época quanto hoje, é que alguns dos ataques

cibernéticos mais destrutivos se tornem mais fáceis de articular com o passar do tempo, e que mais países e outros grupos adquiram as capacidades necessárias para articulá-los.

Logo depois que o US-CCU iniciou seu trabalho, decidimos que precisávamos começar a rastrear as ameaças, bem como suas consequências, para determinar se estávamos investigando os tipos de ataque adequados. Nós nos tornamos muito bons nisso, não nos baseando em ataques já ocorridos, mas observando analiticamente as condições preliminares para os ataques cibernéticos: de que grupos poderiam vir esses ataques em potencial, como e quanto esses grupos poderiam ganhar realizando vários ataques, que alvos pareceriam ser os mais vantajosos para eles, quão difícil e custoso lhes seria reunir as capacidades necessárias, e que sinais estão disponíveis para indicar suas atividades cibernéticas atuais.

Agora estamos oferecendo cursos intensivos de um e dois dias para corporações e órgãos do governo, nos quais ensinamos as técnicas que desenvolvemos para analisar as ameaças de um ataque cibernético e suas consequências. Nossa análise de ameaça cibernética mostra às organizações os métodos e modelos que permitiram ao US-CCU prever todas as novas ameaças cibernéticas significativas desde 2003. Nosso curso de análise de consequências lhes ensina a quantificar coisas como dano às relações com os clientes, dano à marca ou à reputação, e perda de informações de negócio que são importantes em termos competitivos. Também começaremos a oferecer um curso de análise de políticas cibernéticas, demonstrando como quantificar o retorno sobre o investimento e como avaliar comparativamente as diferentes opções. Enquanto isso, o US-CCU continua com suas pesquisas sobre as ameaças atuais e suas consequências.

Você avaliaria como positivo ou negativo que o governo dos Estados Unidos atualmente tenha pelo menos meia dúzia de organizações diferentes lidando com a questão da segurança cibernética?

O governo dos Estados Unidos tem pelo menos meia dúzia de missões muito diferentes envolvendo segurança cibernética. Essas missões impõem demandas conflitantes, e por isso considero apropriado

ter pelo menos meia dúzia de organizações governamentais diferentes lidando com a questão. Infelizmente, essas organizações não têm responsabilidades e capacidades bem alinhadas com as seis missões do governo. Em consequência, temos lacunas, justaposições, disputas de poder e muita confusão sobre quem deveria estar fazendo o quê. Pouco a pouco vamos resolvendo esses problemas, e não creio que o governo consolidará as responsabilidades de segurança cibernética em uma única organização. Acho que atribuirá com mais clareza diferentes tipos de responsabilidade a diferentes organizações. Também haverá uma necessidade cada vez maior de fazer de sua própria segurança cibernética uma responsabilidade explícita de cada departamento e órgão do governo.

O US-CCU realiza pesquisas com foco específico em Talentos e Recursos Humanos? Em caso afirmativo, quais foram as descobertas mais importantes?

Praticamente todos os esforços de pesquisa do US-CCU, desde o início até hoje, sempre mostraram a necessidade de expertise em segurança cibernética em mais lugares. Além disso, acreditamos que, nos programas de capacitação para segurança cibernética, a ênfase quase exclusiva em vulnerabilidades técnicas tem sido nociva à área. Esse foco excessivamente estrito tem limitado a capacidade dos profissionais de segurança cibernética de se comunicar com os de fora da área. Tem impedido a área de ter uma compreensão melhor das ameaças, consequências e políticas. Tem feito que os recursos de nosso país para defesa cibernética, que são limitados, sejam mal alocados, desperdiçando grandes somas de dinheiro e deixando alvos importantes com proteção inadequada. Não só precisamos de mais profissionais capacitados em mais aspectos de segurança cibernética, como também precisamos que praticamente todos os líderes no governo e nos negócios tenham algum preparo rudimentar no assunto. A capacitação em segurança cibernética precisa chegar a uma gama muito mais ampla de executivos e cobrir um leque muito mais variado de materiais.