UMA ESTRATÉGIA PARA A GOVERNANÇA DA SEGURANÇA CIBERNÉTICA NO BRASIL

Por que precisamos falar sobre 'Governança'?

Complexidades relacionadas à segurança cibernética não são novas para o Brasil. O artigo "Uma Estratégia para a Governança da Segurança Cibernética no Brasil" mostra como o país desenvolveu, nos últimos anos, novas instituições e responsabilidades para lidar com os crescentes desafios no âmbito da administração pública federal. No entanto, novas formas de ataque trazem perguntas fundamentais sobre coordenação e cooperação entre diferentes setores. Nesse sentido, a segurança prova-se uma responsabilidade compartilhada e que demanda, a nível nacional, a construção de canais de interlocução entre o governo, setor privado, sociedade civil, academia e comunidade técnica.

A elaboração de políticas e diretrizes nessa área não é exclusiva aos campos da segurança ou defesa nacional, mas faz parte de um processo amplo de governança, que incluem arranjos formais e informais de cooperação entre os diferentes atores. Esta nota estratégica propõe uma estratégia para a governança da segurança cibernética no Brasil, com recomendações e apontamentos sobre as principais lacunas para o diálogo e desenvolvimento de processos participativos tanto para a cooperação política quanto técnica.

Também apresenta:

- Uma análise da arquitetura de governança da segurança cibernética no Brasil, que coloca em perspectiva as principais instituições engajadas nesse processo.
- Uma reflexão sobre os desafios de planejamento e operação para a cooperação nesta área durante o ciclo de megaeventos sediados no país entre 2012 e 2016, bem como seus efeitos na criação acelerada de estruturas na Administração Pública Federal.
- Recomendações para o avanço da cooperação entre os setores envolvidos na segurança cibernética no país.

Como fizemos?

A nota foi elaborada a partir do mapeamento das instituições que compõem o que denominamos estrutura de governança cibernética no país (ver figura). Também contou com a organização de um grupo focal composto por especialistas técnicos e representantes de governo, academia, sociedade civil e setor privado.

O que identificamos?

- A institucionalização da segurança cibernética no Brasil foi impulsionada por dois episódios principais: (i) a aprovação do Marco Civil da Internet, em 2013; e (ii) os megaeventos sediados no país entre 2012 e 2016.
- Os megaeventos resultaram em quatro impactos principais: (i) excessiva securitização e acentuada militarização da segurança cibernética; (ii) exclusão de atores não estatais da definição de temas relevantes para a agenda política; (iii) preferência por soluções como o bloqueio de aplicações e remoção de conteúdo; e (iv) dificuldade de coordenação no âmbito da administração pública federal.
- Esses impactos se refletem nos desafios enfrentados na formulação de políticas para a segurança cibernética, com destaque para: (i) tensões entre abordagens de cunho proibicionista e criminalizante e aquelas focadas na garantia de direitos digitais; (ii) pouca colaboração entre atores do governo, setor privado, sociedade civil e academia envolvidos na formulação de políticas para a área; e (iii) ausência de mecanismos eficazes de colaboração e governança para a segurança cibernética no país.
- O maior desafio para uma governança multissetorial da segurança cibernética é definir papéis e responsabilidades para cada setor. A falta de consenso e de coordenação dificulta a sustentabilidade das políticas.

INSTITUTO IGARAPÉ
a think and do tank

www.igarape.org.br