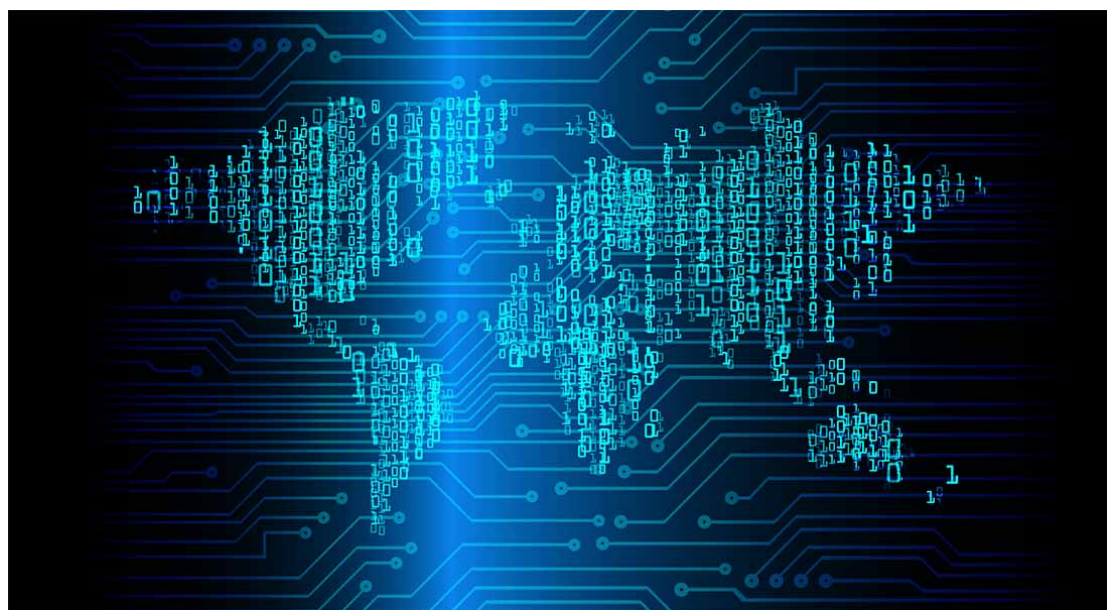


DEFININDO A DIPLOMACIA CIBERNÉTICA

Por Mark Bryan F. Manantan*



The German Marshall Fund of the United States.

A prática diplomática é fundamental para estabelecer as bases para a cooperação entre atores estatais e não estatais dentro de interesses no ciberespaço. No entanto, as abordagens diplomáticas nessa área estão repletas de desafios complicados.

A escala e a velocidade dos avanços tecnológicos no ciberespaço não têm precedentes. Com o amanhecer da quarta revolução industrial, trazendo consigo a realidade do *Big Data*, inteligência artificial e tecnologia quântica, o mundo está entrando em um novo nível de hipoconectividade mais sofisticada, obscurecendo a natureza da interação e troca entre as comunidades *offline* e *online*. O papel da nova fronteira cibernética é significativo pela maneira como os estados-nação conceituam seus interesses no mundo contemporâneo. É uma espécie de calcanhar de Aquiles para os governos que buscam mitigar suas ameaças e, ao mesmo tempo, maximizar as oportunidades que ela oferece. À medida que aumentam as possibilidades de inovação no ciberespaço, também aumenta o potencial de competição e, em certa medida, de conflito.

Os Estados estão gradualmente concentrando sua atenção em mecanismos de política que possam promover e salvaguardar seus interesses no domínio cibernético. Muitos formuladores de políticas que lutam com a incerteza desse território desconhecido também estão cientes da urgência subjacente à necessidade de regras, protocolos e comportamentos compartilhados e aceitos que facilitarão as interações suaves entre os atores globais dentro dele.

Comparado aos domínios tradicionais de terra, ar e mar, onde a diplomacia estabeleceu perfeitamente a base da interação normativa do estado, o ciberespaço é complexo e está em constante evolução. Apesar da noção comum de que o ciberespaço pertence aos bens comuns globais, a cooperação nessa área tem sido fragmentada e *ad hoc*. A natureza intangível e em constante mudança do ciberespaço, que atraiu uma mistura de atores com motivos normativos e ideológicos variados, sugere a necessidade de abordagens diplomáticas multi-ator e coerentes que sejam inovadoras, ágeis e adaptáveis. Assim, o conceito de diplomacia cibernética se tornou uma fronteira emergente para desenvolver a cooperação e a interoperabilidade em um espaço tão disputado.

A diplomacia cibernética é amplamente definida como o uso de ferramentas e iniciativas diplomáticas para alcançar o interesse nacional de um estado no ciberespaço, que são comumente cristalizadas nas estratégias nacionais de segurança cibernética. A diplomacia cibernética abrange uma ampla gama de agendas diplomáticas, como o estabelecimento de comunicação e diálogo entre atores estatais e não estatais; prevenção de uma corrida armamentista cibernética; desenvolvimento de normas globais; e a promoção dos interesses nacionais no ciberespaço por meio de políticas de segurança cibernética e estratégias de engajamento. Também se concentra na evolução das funções dos diplomatas e na reorganização de vários departamentos e ministérios de relações exteriores para atender à crescente proeminência da segurança cibernética na prossecução da política externa ou o papel das novas tecnologias nos processos e estruturas da diplomacia.

A diplomacia cibernética é informada por várias dimensões do poder brando e é considerada uma solução eficaz para mitigar a eclosão de enormes incertezas políticas ou econômicas, riscos e conflitos potenciais provenientes do ciberespaço. Os elementos fundamentais na caixa de ferramentas da diplomacia cibernética são a construção de capacidade cibernética, medidas de fortalecimento da confiança e o desenvolvimento de normas cibernéticas.

A capacitação em segurança cibernética é motivada pelo objetivo final de impedir ameaças. Os estados estão desenvolvendo a capacidade cibernética para reduzir as ameaças relacionadas e convencionais representadas por atores rivais. Envolve a difusão de conhecimentos técnicos, de governança e diplomáticos necessários para garantir a resiliência contra ameaças *online*, abrangendo a implementação de estratégias nacionais de segurança cibernética, o estabelecimento de equipes de resposta a incidentes de computador e o fortalecimento de órgãos de aplicação da lei.

No entanto, as dimensões da construção de capacidade evoluíram além de considerações técnicas padrão ou estruturas regulatórias para incluir o aumento da educação e conscientização. Como a natureza das ameaças cibernéticas não conhece fronteiras, o desenvolvimento de capacidades surgiu para ajudar as economias em desenvolvimento que enfrentam vários desafios de segurança devido à desigualdade ou falta de habilidades e recursos técnicos. Abordar essa condição debilitante requer desenvolvimento de recursos humanos, reforma institucional e organizacional, cooperação público-privada e acesso à própria conectividade com a Internet.

Medidas de construção de confiança (CBMs, do inglês *confidence-building measures*) no domínio cibernético permitem maior compartilhamento de informações para mitigar as incertezas, aumentar a previsibilidade e a transparência nas motivações e intenções e facilitar o gerenciamento de crises ou estratégias de remediação entre os estados. Como as atividades cibernéticas são encobertas pelo sigilo, as CBMs fornecem mecanismos para prevenir e regular certos comportamentos, reduzindo a ambiguidade e a suspeita.

O compartilhamento de informações em CBMs gira em torno do perfil dos atores da ameaça; táticas, técnicas e procedimentos (TTPs), sistemas e divulgações de vulnerabilidades; bem como a publicação de doutrinas cibernéticas e políticas nacionais de segurança cibernética. As CBMs também estão abrindo caminho na promoção de normas cibernéticas, estabelecendo expectativas compartilhadas sobre a conduta aceitável dos Estados-nação, bem como mitigando uma corrida armamentista cibernética no desenvolvimento de capacidades.

As normas cibernéticas são definidas como “padrões de comportamento apropriado em relação ao uso de TIC” no contexto da manutenção da estabilidade e segurança internacionais. São “normas voluntárias e não obrigatórias como uma alternativa à lei”. Por outro lado, o direito internacional pode servir de base para as normas cibernéticas, e as normas cibernéticas podem ser codificadas em direito internacional para conflitos cibernéticos ou guerra cibernética, conforme exemplificado no Manual de Tallinn.

Em meio a ataques cibernéticos crescentes a infraestruturas críticas, violações de dados, crimes cibernéticos, espionagem cibernética, roubo e furto *online* de segredos comerciais e operações cibernéticas ofensivas realizadas por atores estatais ou não estatais, a diplomacia cibernética pode mitigar a agressão cibernética ou a escalada de conflitos. A natureza hiperconectada e transfronteiriça do ciberespaço torna fundamental que os estados se desenvolvam e se envolvam na diplomacia cibernética, em vez de depender exclusivamente da defesa cibernética.

Por meio de iniciativas de capacitação e CBMs, atores estatais e não estatais podem ser capazes de estabelecer uma atmosfera de previsibilidade e transparência. E com a interação constante e colaboração contínua nessas áreas, a potencial criação e adoção de normas cibernéticas que regulam o comportamento do Estado responsável tornam-se viáveis a longo prazo.

A última década viu um aumento no apelo dos Estados por estratégias de diplomacia cibernética mais cooperativas. O mais notável entre esses esforços de diplomacia cibernética foi o Acordo Cibernético EUA-China em 2015, firmado pelo presidente Barack Obama e pelo presidente Xi Jinping. O acordo levou à redução das atividades de espionagem cibernética chinesa, juntamente com uma recalibragem das políticas cibernéticas por parte de Pequim, o que resultou em uma relação cibernética entre os EUA e a China mais amigável.

Além disso, atores não-estatais, incluindo empresas multinacionais e privadas, também estão ativamente envolvidos na diplomacia cibernética. A Microsoft possui sua própria Estratégia de Segurança Global e Equipe de Diplomacia,

enquanto a Huawei tem colaborado com a Microsoft e o East-West Institute para desenvolver padrões para influenciar as aquisições de TIC. Apesar de serem atores subestatais, essas empresas de TIC estão exalando agências diplomáticas para promover as normas cibernéticas.

Mas, apesar do momento positivo na diplomacia cibernética entre atores individuais estatais e não-estatais, as tensões subjacentes no nível multilateral paralisaram a cooperação, especialmente em questões críticas de desenvolvimento de normas cibernéticas e a aplicabilidade do direito internacional no ciberespaço. Há uma contestação crescente entre as democracias ocidentais e os campos autoritários, decorrentes de suas visões divergentes sobre a aplicação do direito à autodefesa, o direito internacional humanitário e o uso de contramedidas no ciberespaço.

Enquanto os EUA defendem a contenção de conflitos baseados em dados cibernéticos, a Rússia e a China estão mais preocupadas em prevenir a ocorrência de conflitos. A Rússia e a China acreditam que os Estados Unidos poderiam usar o direito internacional para justificar o uso de armas cibernéticas no caso de um conflito armado. Os EUA, a Rússia e a China divergem fundamentalmente na identificação da natureza do próprio conflito cibernético.

Há uma divisão fundamental profundamente arraigada entre os EUA e seus aliados contra a Rússia e a China, baseada em suas tendências ideológicas divergentes no aspecto mais amplo da governança da Internet. Por um lado, as democracias ocidentais lideradas pelos EUA defendem uma abordagem de múltiplas partes interessadas que defende a inclusão da participação na promoção e adoção de normas e regras internacionais, particularmente o livre fluxo de informações.

Por outro lado, a Rússia e a China estão mais preocupadas em manter o controle das informações para o bem da segurança nacional, o que se enquadra em sua noção de soberania cibernética. Essa divisão crescente, portanto, é um caso forte para a potencial balcanização da Internet, marcada pelo aumento das fronteiras digitais entre aqueles que defendiam a soberania cibernética e o fluxo livre e aberto de informações.

A lógica subjacente ao fenômeno denominado “Splinternet” também revela a batalha latente pela supremacia tecnológica global entre os EUA e a China. Não é segredo que a China continua avançando em seus esforços no estabelecimento de padrões de tecnologia para desafiar e eventualmente substituir as regras e princípios que governam a Internet, que foram predominantemente estabelecidos e influenciados pelos Estados Unidos. Se for bem-sucedida, isso pode levar à proliferação da infraestrutura descentralizada da Internet, dando origem a uma versão “Ocidental” e “Oriental” do ecossistema da Internet.

Portanto, o caminho para o desenvolvimento de normas cibernéticas que promovam e preservem um ciberespaço mais estável e seguro permanece desolado. Como as relações atuais entre os EUA, China e Rússia continuam a se deteriorar, o ímpeto para as grandes potências virem à mesa não está à vista. Isso torna a perspectiva de cooperação entre os guardiões percebidos do domínio

cibernético altamente implausível e, portanto, desafia o argumento de que as normas cibernéticas apresentam o caminho mais realista para lidar com ameaças cibernéticas.

Reconhecendo a incerteza e os desafios no progresso da formulação de normas cibernéticas internacionais, agravados pelas ameaças em evolução e vulnerabilidades em constante mudança no ciberespaço, os Estados estão criando uma panóplia de ferramentas e iniciativas diplomáticas no ciberespaço com ênfase crescente na dissuasão cibernética.

Artigo publicado no [Australian Institute of International Affairs](#).

****Mark Bryan F. Manantan** é atualmente bolsista no Fórum do Pacífico e bolsista não residente no Centro de Estudos do Sudeste Asiático da Universidade Nacional de Chengchi em Taiwan. Recentemente, ele trabalhou no Centro para Estratégias de Criação de Regras na Tama University em Tóquio, Japão, e no Centro Leste-Oeste em Washington.*
