LA/CS NET

RESUMO DO EVENTO

Simpósio Latino-Americano de Pesquisa em Cibersegurança. Questionando vieses, construindo pontes

Março 2023

Esta publicação foi produzida no contexto do projeto EU Cyber Direct – EU Cyber Diplomacy Initiative com a assistência financeira da União Europeia e da Rede Latino-Americana de Pesquisa em Cibersegurança. O conteúdo deste documento é de responsabilidade exclusiva dos autores e não pode, em nenhuma circunstância, ser considerado como refletindo a posição da União Européia, da LA/CS Net ou de qualquer outra instituição.

A Rede LA/CS agradece a todos os membros e colaboradores que comentaram as versões anteriores deste relatório.

Elaboração do relatório
Louise Marie Hurel (fundadora, LA/CS Net)

Notas do Simpósio
Nils Berglund (EU Cyber Direct)

Equipe Organizadora
Louise Marie Hurel (LA/CS Net)
Nils Berglund (EU Cyber Direct)
Patryk Pawlak (EU Cyber Direct)

Tradução
Ismael Deus Marques (versão em língua portuguesa)

Organizações que implementam EU Cyber Direct:

EU Institute for Security Studies
Carnegie Endowment for International Peace
Leiden University

Financiado pela União Europeia

Índice

Resumo

O primeiro Simpósio Latino-Americano de Pesquisa em Cibersegurança foi realizado no dia 27 de outubro no Ministério das Relações Exteriores do governo do México. O Simpósio foi co-organizado pelo Programa EU Cyber Direct do Instituto Europeu de Estudos de Segurança e pela Rede Latino-Americana de Pesquisa em Cibersegurança (LA/CS Net) e ocorreu como um evento paralelo ao VI Encontro da Organização dos Estados Americanos Grupo de Trabalho de Medidas de Fortalecimento da Confiança. A ocasião também marcou o lançamento oficial da LA/CS Net como plataforma de diálogo, cooperação e pesquisa para cibersegurança na região.

O Simpósio foi a primeira atividade da LA/CS Net e buscou reunir uma comunidade de pesquisadores, acadêmicos e profissionais que trabalham com cibersegurança na América Latina. O objetivo do Simpósio é: (1) facilitar um diálogo para o pensamento crítico sobre uma abordagem culturalmente sensível às agendas de pesquisa neste campo, (2) abrir o espaço para colaborações intersetoriais na região e (3) promover diálogos interdisciplinares.

Durante o evento, especialistas discutiram as oportunidades e os desafios para a consolidação de uma agenda latino-americana de pesquisa em cibersegurança. Este relatório apresenta a LA/CS Net, um resumo da discussão realizada durante o Simpósio, bem como um horizonte de futuras atividades para a Rede. Longe de ser exaustivo, o relatório é um primeiro passo para o desenvolvimento de um diálogo diverso e contínuo sobre o que significa discutir e pesquisar cibersegurança na América Latina e contribuir para uma discussão mais ampla sobre cibersegurança em países em desenvolvimento e no Sul Global.

LA/CS Net: uma plataforma para pesquisa em cibersegurança na América Latina

Ao longo das últimas décadas, a pesquisa em cibersegurança tornou-se um esforço multidisciplinar. Estudiosos de Direito, Relações Internacionais, Ciência Política, Economia Política, Mídia e Comunicações, estudos de Ciência e Tecnologia e muitos outros têm procurado testar os limites dos métodos e conceitos disciplinares para estudar dinâmicas emergentes associadas às inseguranças digitais.

No entanto, apesar da expansão da literatura e interdisciplinaridade do campo, parte da agenda de pesquisa sobre cibersegurança foi moldada por "problemas de segurança" associados aos países desenvolvidos. Embora essas preocupações tenham ajudado a trazer à tona novas questões de segurança associadas ao ciberespaço, elas criaram uma linguagem e um molde de discurso que muitas vezes são transpostos para países em desenvolvimento sem a devida contextualização e sensibilidade cultural.

Longe de tentar ser exaustiva, a investigação sobre a cibersegurança na América Latina associou-se com pressupostos gerais, como: foco no cibercrime e a profissionalização do crime organizado online bem como com as posições "ambíguas" ou "pendulares" dos países em discussões multilaterais, por exemplo.

No entanto, incidentes cibernéticos recentes e de grande notoriedade, como o ransomware Conti na Costa Rica, e as altas taxas de crimes cibernéticos ao longo dos últimos anos ressaltam como a região não está imune aos desafios políticos enfrentados por países desenvolvido. Esses e outros eventos também apontam para a necessidade de uma análise específica dos desafios da cibersegurança na região. Além disso, essas dinâmicas destacam como os binômios Norte-Sul, "em desenvolvimento"-"desenvolvido" e entre outros usados para descrever políticas e pesquisas neste campo, são mais complexos do que se presume e merecem uma análise aprofundada.

Isso ocorre principalmente pois uma "visão ocidental" do cenário de ameaças proporcionou um reconhecimento seletivo de conceitos, noções de ameaças, práticas e conhecimentos que se desenvolveram em outros lugares. Seguem abaixo duas consequências:

- Em primeiro lugar, os países que não estão incluídos no nexo das grandes potências (Sul Global, países em desenvolvimento, Estados pendulares) muitas vezes podem ser definidos em suas comparações com essas referências internacionais, ao invés de serem posicionados e compreendidos em seus respectivos contextos socioculturais.

- Em segundo lugar, uma visão de ameaça referenciada no Norte também contribuiu para a reprodução da lógica da opção binária na literatura – na qual os países latino-americanos só podem convergir ou divergir dessa linguagem, agenda, percepção de problemas de segurança e de respostas. Essa lógica binária ofusca as complexidades institucionais, políticas, econômicas e sociais que compõem o panorama da literatura sobre cibersegurança dos países latino-americanos.

Ciente da necessidade de maior sensibilidade na reflexão sobre os diferentes limites e contingências para a prática e pensamento de cibersegurança na região, surgiu a ideia da LA/CS Net. O objetivo desta iniciativa é construir uma rede de especialistas, dar visibilidade ao que foi produzido até agora e promover diálogos com outras partes interessadas, para informar novos caminhos para colaboração, bem como aprimorar pesquisas baseadas em evidências e contextualmente ricas.

O objetivo do Simpósio foi o de provocar discussões e questionamentos sobre os pressupostos e vieses que cercam a pesquisa em cibersegurança na região, unir comunidades de pesquisadores e iniciar um diálogo e reflexão crítica para o desenvolvimento de uma agenda de pesquisa para o estudo da cibersegurança latino-americana.

Trilhando caminhos: uma agenda de pesquisa para a cibersegurança na América Latina

O Simpósio reuniu 19 participantes de 11 países. A agenda foi dividida em duas partes: A primeira sessão discutiu os desafios e oportunidades para a agenda de cibersegurança na região. A segunda parte concentrou-se na identificação e compartilhamento de lições aprendidas entre acadêmicos e profissionais sobre o processo de condução de pesquisas nessa área. Os participantes concordaram que o Simpósio foi fundamental para organizar e identificar as questões teóricas, conceituais, metodológicas, políticas e práticas para uma agenda de pesquisa. Sendo este, apenas o início do esforço de se pensar coletivamente com estudiosos latino-americanos, uma agenda de pesquisa sobre cibersegurança na e da região.

As seguintes áreas-chave foram identificadas durante a discussão.

Desafios Estruturais

A cibersegurança não está isolada das condições sociais, políticas e econômicas. Os participantes destacaram uma série de desafios para o estudo da cibersegurança na América Latina que vão desde questões sobre financiamento, até considerações conceituais sobre as relações Norte-Sul na pesquisa sobre (e desde) a região.

Financiamento Os desafios relativos ao financiamento não são exclusivos da região, mas na América Latina isso ocorre de maneiras específicas. Os participantes notaram que os fluxos de financiamento geralmente são focados em países específicos. Grande parte das pesquisas acadêmica em humanidades e ciências sociais dependem quase inteiramente de fundos governamentais. Tais desafios também estão ligados a outros fatores estruturais. A falta de senso de regionalidade também significa que há menos incentivos de financiamento para a integração acadêmica inter-regional. Embora existam alguns programas de intercâmbio e cooperação entre universidades, a integração da pesquisa regional em termos de financiamento é a exceção e não a norma. Além disso, há poucos incentivos para pesquisas interdisciplinares em cibersegurança, devido aos rígidos fluxos de financiamento vinculados a disciplinas específicas.

Silos disciplinares Os participantes observaram que a clivagem entre as disciplinas é construída tanto institucional quanto conceitualmente. Institucionalmente, os Ministérios da Educação e as próprias universidades encontram-se restritos a uma perspectiva disciplinar e profissional estreita, linear. Ainda assim, existe espaço para mapear os cursos de cibersegurança em toda a região para identificar melhor em quais departamentos eles estão localizados. Conceitualmente, os participantes observaram que as barreiras entre abordagens técnicas/políticas ou sociais para a pesquisa em cibersegurança derivam dessas restrições estruturais baseadas em disciplinas estanques. Isso, por sua vez, restringe os tipos de questões de pesquisa, métodos, abordagens e dados que podem ser usados para conduzir pesquisas sobre cibersegurança.

Ênfase temática A militarização da cibersegurança foi um dos temas-chave da discussão e identificada como uma característica tanto do desenvolvimento institucional quanto da literatura acadêmica de diferentes países da região. Três preocupações associadas à militarização foram apresentadas: primeiro, o legado preocupante de ditaduras na América Latina e como esse legado se cruza com a concentração de recursos de cibersegurança e defesa dos Ministérios da Defesa. Em segundo lugar, os participantes observaram que, em contextos de militarização da pauta de cibersegurança, torna-se difícil acompanhar as diferenças entre segurança e defesa cibernética. Em terceiro lugar, outros argumentaram que a ideia do ciberespaço como um "quinto domínio" pelos EUA teve implicações institucionais, políticas e teóricas – a militarização sendo uma delas. Existem consequências para o enquadramento da Internet e do ciberespaço como um domínio de guerra tais como a associação da Internet como um espaço de ameaças híbridas, de guerra de informação e entre outros termos.

Emaranhada com a militarização do ciberespaço está a proteção da democracia. Como observou um participante, a democracia foi apresentada durante o evento como "o ativo mais importante e mais difícil de proteger" quando se trata de cibersegurança. A militarização do ciberespaço representa um desafio para a democracia na América Latina, em parte devido à crescente falta de transparência dentro do exército e outras instituições responsáveis pela defesa cibernética, bem como, em alguns casos, devido a retrocessos nas legislações de acesso à informação.

Desenvolvimento linear e mensuração de capacidades Outro aspecto que não se restringe à cibersegurança, mas que tem sido cada vez mais definido como padrão, refere-se à linearidade do entendimento sobre desenvolvimento de capacidades em cibersegurança. Essa agenda deriva em grande medida de uma mentalidade baseada em soluções que tem sido cada vez mais justificada por tentativas de mensurar desenvolvimento no âmbito da cibersegurança. Esses instrumentos, apesar de úteis, podem muitas vezes reforçar as disparidades e servir como justificativas para novas intervenções dos países desenvolvidos com base em seus parâmetros. No entanto, as ferramentas de medição e avaliação não foram vistas como negativas em geral. Alguns participantes sugeriram que os formuladores de políticas deveriam ter uma perspectiva mais clara sobre os mecanismos e modelos de avaliação de capacidades no âmbito nacional – e uma perspectiva que pudesse refletir as particularidades culturais do país.

Entrelaçamentos Regionais e Globais

A América Latina não está posicionada em um vácuo global, pelo contrário, existem camadas de complexidades no posicionamento desses países que precisam ser melhor avaliadas. Durante as discussões, três camadas foram identificadas.

Intrarregional Embora o termo 'América Latina' seja frequentemente usado para se referir a países da América do Sul e outros países de língua espanhola na América Central, a noção de regionalidade não é uma constante na história da região – outras fronteiras, como idioma e tamanho dos países, afetam igualmente o debate sobre cibersegurança na região e, portanto, a literatura e o espaço para cooperação. Futuras pesquisas devem considerar como essas noções fragmentadas e controversas de identidades regionais/nacionais se explicitam na cibersegurança.

Sul-Sul Os participantes reconheceram que ainda há um incipiente intercâmbio e discussão sobre cibersegurança entre os países do Sul, tanto do ponto de vista de projetos políticos quanto acadêmicos.

Norte-Sul As contingências e entrelaçamentos entre Norte e Sul foram um dos principais temas discutidos. Embora os participantes concordassem que é necessário pensar em uma agenda de pesquisa para a América Latina que atenda às realidades dos contextos sociais, econômicos e culturais desses países, eles também observaram que a cibersegurança na região é contingente e entrelaçada com o "Norte Global" de diversas formas. Uma questão apresentada durante as discussões foi:

É possível separar o "Norte" do "Sul" ao pensar em uma agenda de pesquisa latino-americana para cibersegurança?

- A maior parte dos participantes concordaram que é um desafio separar ambos (Norte e Sul). Isso não é exclusivo da cibersegurança, mas tem efeitos específicos e pontos de conexão específicos que vão desde fluxos de financiamento entre Norte/Sul na agenda de capacitação cibernética, o lugar de diferentes acadêmicos do Sul no Norte, e entre outros elementos que codificam uma complexa coexistência entre ambos.
- Alguns observaram que existem agendas e narrativas de segurança específicas presentes em países do 'Norte' que são projetadas no 'Sul' e, especificamente, na América Latina. Um exemplo refere-se a preocupações sobre a interferência russa ou influência chinesa em processos eleitorais. Embora possa ser esse o caso, os países da região podem estar mais preocupados com grupos domésticos ou com questões de segurança pública ligadas ao crime organizado online.
- Outros destacaram que o vocabulário e os conceitos utilizados para abordar problemas de cibersegurança concentram-se em termos em inglês – ex: Como rotulamos as violações de dados (data breach)? Países possuem suas respectivas abordagens e terminologias. É desejável e realista considerar um vocabulário propriamente nacionalizado em um contexto no qual a natureza das ameaças à cibersegurança permanecem profundamente interligadas a um ambiente global/transnacional no qual o inglês é a língua franca? Contudo, há casos em que o inglês pode fornecer maiores nuances às ameaças (por exemplo, security/safety é a mesma palavra em espanhol/português e sua distinção para pesquisa em cibersegurança é significativa).
- Uma vez que o inglês nos proporcionou um vocabulário como plataforma para discutir cibersegurança (academicamente, politicamente e no âmbito da indústria), torna-se desafiador ignorar completamente esses efeitos sistêmicos dessa consolidação - "Não podemos realmente parar de usar o dólar ou o inglês como idioma global, então podemos desconectar o norte global do sul global? Deveríamos?"

Navegando o Campo: a prática de se "conduzir" a pesquisa

O segundo painel do Simpósio Latino-Americano de Pesquisa em Cibersegurança foi dedicado exclusivamente a uma discussão sobre os aspectos práticos e os desafios para a realização de pesquisas sobre cibersegurança na região. Este debate contou com reflexões e experiências de profissionais de organizações da sociedade civil, como Red de Defensa de los Derechos Digitales (R3D) – um think tank baseado no México envolvido em negociações e agendas políticas sobre cibersegurança no âmbito nacional e internacional.

Como pesquisadores e organizações da sociedade civil podem engajar com agendas internacionais e, ao mesmo tempo, garantir o espaço para regionalidades, e debates contextualizados?

É difícil evitar que a estrutura da pesquisa seja 'de cima para baixo', tanto em nível regional quanto em relação ao norte global, que define o tom e a agenda da pesquisa em cibersegurança. Precisamos de abordagens mais contextualizadas, regionalizadas e nacionalizadas.

Sigilo na pesquisa e na prática—O que é necessário para construir um relacionamento e navegar as contingências (históricas, políticas, partidárias, de gênero) da pesquisa em cibersegurança na América Latina?

Governos Muitos governos não estão dispostos a compartilhar documentos com pesquisadores – ou incluí-los no processo de desenvolvimento de políticas – especialmente quando as agendas de cibersegurança abordam preocupações de segurança nacional. Diversas explicações são aplicáveis a essa afirmação, mas ainda assim,

requerem maiores análises sobre as contingências entre o governo e a academia. O histórico de ditaduras militares na América Latina, por exemplo, deixou um legado de desconfiança e desconforto entre os civis e as forças armadas – e por mais que tenham terminado, a divisão ou atrito cultural permanece. Em países onde a cibersegurança é amplamente militarizada (por exemplo, Brasil), essa desconfiança com a sociedade civil e o terceiro setor é frequentemente observada – com algumas exceções. Isso é agravado por uma falta geral de informações (retrocesso nas leis de acesso à informação), poucas proteções para pesquisadores de segurança e políticas nacionais que tornam a pesquisa um desafio (por exemplo, o México tem um 'código criminal mal escrito', onde muitos aspectos da pesquisa são essencialmente criminalizados – conforme apontado por um dos participantes).

Alguns participantes observaram que muitas vezes é mais fácil (do ponto de vista do estabelecimento de um diálogo/relacionamento) para organizações da sociedade civil conduzirem advocacy no âmbito internacional devido às oportunidades de acesso a representantes que elas obtêm em fóruns multilaterais como a ONU. Um exemplo levantado durante a discussão foi o do México. Por um lado, no âmbito internacional, o país ativamente busca o envolvimento de várias partes interessadas nos diálogos sobre cibersegurança. Apesar de tal reconhecimento e diálogo, destacou-se que as delegações da ONU não refletem a estrutura nacional, onde as organizações da sociedade civil têm dificuldade em estabelecer interlocuções com instituições governamentais locais e nacionais no desenvolvimento de políticas. É importante evidenciar e refletir sobre essas contradições domésticas/internacionais e, ao mesmo tempo, aproveitar os espaços internacionais para construir pontes com outras organizações do terceiro setor e trocar experiências.

Setor privado Os participantes observaram que há pouca transparência por parte do setor privado sobre ameaças na região – o que, por sua vez dificulta acesso a dados para pesquisa em cibersegurança na América Latina. Embora em áreas temáticas correlatas como operações de informação e influência novos modelos de compartilhamento de dados e cooperação com a comunidade de pesquisa tenham sido desenvolvidos, a pesquisa em cibersegurança se beneficiaria de um maior diálogo com empresas nacionais e internacionais que trabalham na região. Isso fomentaria maiores reflexões e literatura sobre o cenário de ameaças, bem como traria maior visibilidade sobre as especificidades e semelhanças de ameaças, atores e práticas na América Latina.

A questão dos dados também levanta o desafio da responsabilidade das empresas. Como observaram os participantes, "eles [big tech] definem normas, exercem poder e influenciam... mas não têm responsabilidade sobre o uso e distribuição de dados". Os marcos legais são muito específicos e feitos em nível nacional, "(...)mas a Meta e o Twitter são empresas norte-americanas sujeitas a um marco legal norte-americano – e não temos normas internacionais que regem as empresas. Qual é a relação e a responsabilidade do setor privado com o direito internacional? E as obrigações de denunciar hacks?"

Pontos adicionais *O dilema do pesquisador:* Com uma quantidade considerável de pesquisas sobre cibersegurança (especialmente de uma perspectiva de ciências humanas e sociais) sendo produzidas (e tornada mais visível) em universidades da Europa, Reino Unido e EUA, os pesquisadores da região enfrentam o desafio de como navegar e equilibrar os incentivos do 'capital social' de falar, posicionar e escrever em periódicos nessas regiões/países' vis-à-vis uma agenda menos centrada no inglês.

A 'localização desconhecida' da cibersegurança na América Latina: Quais são os espaços para se pesquisar cibersegurança na América Latina? Por um lado, muitas vezes há uma competição entre processos (por exemplo, IETF x ISOC; UNCTAD x OMC) que fala sobre o surgimento de "múltiplos multilateralismos" nas agendas digital e cibernética. Por outro lado, mais pesquisas são necessárias para entender onde e quais dimensões da cibersegurança estão sendo abordadas em mecanismos regionais (por exemplo, OEA) e outros fóruns relevantes desde a perspectiva dos países latino-americanos.

A necessidade de uma visão mais ampla

Os países da América Latina sabem o que eles desejam quando se trata da agenda de cibersegurança? As preferências são tão importantes quanto às capacidades, ex: não apenas o que um país pode fazer, mas também o que um país deseja fazer (suas ambições? Valores?). Conforme participantes apontaram, o avanço de normas

para cibersegurança deve estar aliada a um discurso público e transparente sobre o que um estado/país deseja alcançar. Um desafio para entender como a soberania funciona na América Latina, por exemplo, é que muitos países não têm uma posição formada sobre as normas cibernéticas. Maior transparência é fundamental não só pela perspectiva da responsabilidade dos Estados em proteger e garantir a paz no ciberespaço, mas também por uma perspectiva de preferências (ou seja: entender se os Estados veem a cibersegurança como um problema de segurança nacional ou um problema de segurança pública? Se ambos, como eles interagem?)

- Observou-se que os Estados latino-americanos têm sido relativamente bem-sucedidos quando se trata da organização/respostas ao cibercrime. A convenção de Budapeste tem sido um ponto central para o desenvolvimento de normas e cooperação técnica entre políticas, ministérios da justiça, e entre outros mecanismos.

- Ao mesmo tempo, diferentes agências/ministérios competem (por vezes) uns com os outros para obter recursos em questões de digitalização e cibersegurança – muitas vezes criando barreiras ao diálogo interministerial. Isso também cria desafios de transparência e acesso à informação para pesquisadores/organizações da sociedade civil.

Melhorar a colaboração inter-regional entre pesquisadores e partes interessadas. A pesquisa sobre cibersegurança se beneficiaria de mais conexões entre regiões. A Rede LA/CS é uma plataforma para facilitar o diálogo entre pesquisadores que estudam a América Latina. Um dos objetivos desse esforço é de aumentar as colaborações e os laços de pesquisa na região, mas potencialmente com outras regiões e em especial com outros pesquisadores do Sul Global. Além disso, a Rede também buscará aprimorar os diálogos entre pesquisadores e outros setores para fortalecer a cooperação para o desenvolvimento de pesquisas informadas e baseadas em evidências.

Ampliando a pesquisa e os intercâmbios interdisciplinares. Há uma necessidade de reavaliar as metodologias de pesquisa ao pensar em dados e acesso a informações. Quais metodologias e fontes estão à disposição para pesquisadores estudarem temas como diplomacia (na área de cibersegurança) ou inteligência de ameaças? Como identificar contatos-chave em diferentes setores na condução da pesquisa? Quais são as nuances de se envolver em advocacy durante a realização de pesquisas acadêmicas? Os pesquisadores reconheceram que há uma oportunidade para a LA/CS Net facilitar diálogos sobre diferentes métodos (pesquisas, etnografia, observação participante e outros) com vistas a diversificar o presente enfoque em análise de documentos ou dados secundários – um método e fonte comum usado por estudiosos na área de Humanidades.

'Cegueira de dados'? Novas perguntas, novos conjuntos de dados, novas parcerias. Precisamos construir novos conjuntos de dados que contribuam para o mapento do panorama de ameaças na América Latina, melhorem a integração dos indicadores de ameaças e facilitem uma reflexão crítica sobre ameaças relevantes. Atualmente, a América Latina não aparece nos conjuntos de dados sobre ameaças e ataques/incidentes, pois eles geralmente dependem de algoritmos de coleta de notícias que priorizam o idioma inglês e os meios de comunicação no Norte Global.

Conclusão

A América Latina é diversa, complexa e muito mais do que uma região geográfica. O Simpósio Latino-Americano de Pesquisa em Cibersegurança demonstrou que a condução de pesquisas sobre a região combina uma série de dimensões. Inclui o entrelaçamento entre Norte e Sul, o posicionamento da América Latina na noção mais ampla de 'Sul' e a relação entre os países latino-americanos e a noção de regionalidade. Por mais que nenhuma dessas dimensões sejam 'novas', elas têm repercussões específicas para o estudo da cibersegurança que igualmente carece de maior aprofundamento.

As discussões mostraram que há uma oportunidade de fortalecer o diálogo em torno de medidas práticas sobre a condução de pesquisas sobre segurança cibernética. Faz-se necessário, portanto, de posicionar a pesquisa em cibersegurança vis à vis questões de linguagem (idioma), acesso, privilégio, tecnicidade, posicionalidade de

stakeholders e entre outras barreiras que se apresentam de maneiras específicas, dependendo da disciplina e do país em que se está conduzindo sua pesquisa.

Mais importante ainda, o Simpósio mostrou que o esforço de construção de uma agenda de pesquisa em cibersegurança na região está longe de ser um exercício pontual, mas é apenas o início de um diálogo contínuo. Mostrou também que existe um espaço frutífero para um diálogo crítico não apenas dentro da região, mas de como ela se conecta com um esforço geral de avanço da pesquisa Sul-Sul em cibersegurança.

Sobre EU Cyber Direct – EU Cyber Diplomacy Initiative

EU Cyber Direct – EU Cyber Diplomacy Initiative apoia a diplomacia cibernética da União Europeia e os compromissos digitais internacionais, a fim de fortalecer a ordem baseada em regras no ciberespaço e construir sociedades resilientes cibernéticas. Para isso, realizamos pesquisas, apoiamos o desenvolvimento de capacidades em países parceiros e promovemos a cooperação multissetorial. Por meio de pesquisas e eventos, o EU Cyber Direct se envolve regularmente nas discussões sobre o futuro da cooperação internacional para combater o cibercrime e fortalecer os sistemas de justiça criminal globalmente.

Para saber mais, visite o site do projeto www.eucyberdirect.eu ou entre em contato com **Nils Berglund**, coordenador de divulgação e engajamento público, nils.berglund@iss.europa.eu.

Sobre Latin American Cybersecurity Research Network

A Latin American Cybersecurity Research Network (LA/CS NET) é uma iniciativa dedicada a mapear, conectar e aprofundar o trabalho acadêmico em e de países da região. A Rede busca reunir acadêmicos de dentro e fora da região que realizam pesquisas em segurança cibernética na América Latina e fornecer mais visibilidade aos cenários, teorias e conceitos de ameaças nesses contextos específicos.

Para saber mais sobre a Rede, visite o site da LA/CS Net www.latamcyber.net ou entre em contato com a iniciativa aqui.