RNP Educação, Pesquisa e Inovação em Rede

Relatório de Visão de Futuro

Comitê Técnico de Cibersegurança

maio de 2025

Coordenador do CT-Cibersegurança

Igor Monteiro Moraes (UFF)

Coordenador Adjunto do CT-Cibersegurança

Ian Vilar Bastos (UERJ)

Coordenador da RNP para o CT-Cibersegurança

Reinaldo Cézar de Morais Gomes (RNP)

Assessor Acadêmico-Científico

José Ferreira de Rezende (RNP/UFRJ)

Diretora de Pesquisa e Desenvolvimento

Iara Machado (RNP)

Autores

André Ricardo Abed Grégio (UFPR)
Diogo Menezes Ferrazani Mattos (UFF)
Edmar Candeia Gurjão (UFCG)
Ian Vilar Bastos (UERJ)
Igor Monteiro Moraes (UFF)
Miguel Elias Mitre Campista (UFRJ)
Reinaldo Cézar de Morais Gomes (RNP)

SUMÁRIO

1 Introdução

Os avanços tecnológicos impulsionam a humanidade em direção a uma sociedade cada vez mais virtual e conectada. Porém, tais avanços também abrem brechas a ciberataques que visam oferecer vantagens a quem não for de direito ou prejuízos a operação de sistemas. Entre tais prejuízos estão a paralisação das operações de sistemas críticos e grandes empresas, a invasão de privacidade de instituições ou indivíduos, o acesso não autorizado ou roubo de recursos e até mesmo o mau uso de propriedades intelectuais com potencial de dissidência entre países ou organizações. Nesse sentido, muitos esforços são envidados para produzir sistemas mais seguros ou aumentar a segurança dos já existentes, que podem sofrer com falhas não previstas, revisitando discussões sobre o compromisso entre prevenção e correção. Esses esforços se refletem na valorização dos profissionais de cibersegurança, cujos salários devem aumentar em até 33% de 2023 até 2033, segundo estatísticas (U.S. BUREAU OF LABOR STATISTICS, 2025). E ainda assim há um déficit de 750 mil profissionais de cibersegurança, somente no Brasil (FORTINET, 2024).

A RNP, como vanguardista nacional em tecnologia, deve acompanhar os avanços em cibersegurança, tendo em vista o seu compromisso na prestação de serviços de infraestrutura para pesquisa a instituições de ensino e pesquisa de todo o país. A RNP deve manter o uso correto de sua infraestrutura e a privacidade dos seus usuários. Dessa forma, torna-se imperativo investir em cibersegurança com base em uma análise criteriosa feita por especialistas na área. Este é o primeiro passo dado pelo CT-Cibersegurança, cujo papel é acompanhar a evolução, prospectar soluções tecnológicas e apresentar recomendações técnicas, em caráter consultivo, para a RNP na área de cibersegurança. O CT-Cibersegurança propõe, portanto, um documento de visão de futuro com o objetivo de identificar os temas em evidência na área tanto sob o ponto de vista da academia quanto da indústria. O documento foi construído usando uma metodologia criteriosa para busca das principais tendências na área tanto sob o ponto de vista da academia, via conferências de destaque, quanto na indústria, obtida pela busca por iniciativas nacionais e internacionais. O documento ainda faz projeções em três horizontes de tempo, associado um fator temporal às tendências encontradas. As tendências no primeiro horizonte de tempo envolvem aplicações de grandes modelos de linguagem para, por exemplo, criação de relatórios de inteligência automatizados, análise de código-fonte em busca de vulnerabilidades e criptanálise. Além disso, há uma necessidade urgente de ações para fomentar a educação em cibersegurança dado a enorme escassez de profissionais capacitados para atuar na área. No segundo horizonte, as tendências identificadas estão relacionada ao uso de arquiteturas de confiança zero (*Zero Trust*) e Inteligência Artificial Generativa, que pode ser aplicada à geração de políticas e automação avançada de soluções de cibersegurança ou automatizar análises de forense digital. No terceiro horizonte, as tendências incluem criptografia pós-quântica, avanços em hardware para detecção antecipada de ameaças e centros de operação de segurança quase que totalmente gerenciados por inteligência artificial.

O restante deste documento está organizado da seguinte forma. A Seção 2 descreve as etapas da metodologia usada para definição dos horizontes de tempo e identificação de tendências em cibersegurança. A Seção 3 apresenta os resultados da análise dos dados de conferências renomadas da área de cibersegurança que nortearem a identificação das tendências. As Seções 4 e 5 identificam iniciativas nacionais e internacionais na área de cibersegurança, incluindo grupos de pesquisa que atuam na área, projetos científicos e suas fontes de financiamento, teses e dissertações e patentes e registros de software. A Seção 6 apresenta as tendências identificadas para os três horizontes que definem a visão de futuro deste documento. Por fim, a Seção 7 conclui este documento.

Escopo

O escopo desse documento se limita a identificar tendências tecnológicas relacionadas à cibersegurança e que possam servir para nortear atividades de pesquisa, desenvolvimento e inovação na

área em curto, médio ou longo prazo. Uma vez que o presente documento tem como público-alvo o sistema RNP, considerou-se aquelas tendências na academia e na indústria que possam gerar evoluções para os serviços oferecidos pela RNP, bem como fomentar novos serviços ou modelos de negócio. Assim, este documento não é uma revisão extensiva da literatura ou de análise completa e esgotada dos tópicos relacionados com cibersegurança.

2 Metodologia

A metodologia utilizada neste relatório está ilustrada na Figura 1, consistindo em cinco etapas principais: estabelecimento da janela de tempo; estabelecimento das fontes de dados; preparação dos dados; análise dos dados e das tendências; e identificação de horizontes e mapeamento dos temas.

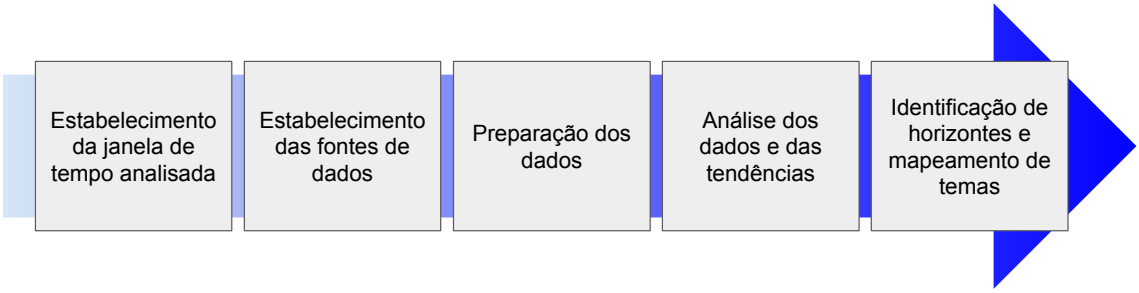


Figura 1: As cinco etapas da metodologia utilizada neste relatório de visão de futuro.

Estabelecimento da janela de tempo: A janela de tempo estabelecida para pesquisa do estado da arte e das iniciativas nacionais e internacionais em P&D em cibersegurança é de cinco anos, i.e., de 2020 até 2024. Tal janela foi discutida e definida em reunião plenária *online* como uma solução de compromisso, que busca identificar as tendências com base em publicações e outras iniciativas de passado recente.

Estabelecimento das fontes de dados: As fontes de dados foram divididas em duas principais. Para o estado da arte, determinou-se o uso das top-10 conferências conforme lista da CESeg[1] mais o Simpósio Brasileiro de Cibersegurança (SBSeg), por se tratar da principal conferência nacional da área. Essa lista também foi definida em reunião plenária *online* deste comitê técnico e pode ser vista na Tabela 1, junto com sua posição no ranqueamento da CESeg e da URL típica do evento. Considerando tais eventos, a base de dados foi construída com os títulos dos artigos publicados e os títulos das sessões técnicas correspondentes nas trilhas principais de cada evento. A base de dados usada no levantamento do estado da arte considerou os *sites* de cada evento e a programações técnicas disponíveis publicamente nestes *sites*. Para o panorama nacional, determinou-se o uso do Diretórios de Grupos de Pesquisa do CNPq para identificar grupos de pesquisa em cibersegurança no Brasil, das bases de dados de dissertações e teses da CAPES para identificação de temos de pesquisa em cibersegurança nos quais os grupos de pesquisa trabalham e das bases de dados do INPI para identificar patentes depositadas e *softwares* registrados por pesquisadores brasileiros em cibersegurança. Para o panorama internacional, determinou-se o uso de bases de dados de projetos financiados pela National Science Foundation, nos EUA, e de projetos europeus financiados pela Comissão Europeia.

[1] Disponível em https://www.ceseg.org/onde-publicar.

Tabela 1: Conferências usadas para criação da base de dados.

Posição	Título da conferência	URL padrão ou da última edição
1	ACM Symposium on Computer and Communications Security (ACM CCS)	https://www.sigsac.org/ccs/CCS2024/
2	IEEE Symposium on Security and Privacy (IEEE S&P)	https://sp2024.ieee-security.org
3	USENIX Security Symposium (USENIX Security)	https://usenix.org/conference/usenixsecurity24
4	International Cryptology Conference (CRYPTO)	https://crypto.iacr.org
5	Network and Distributed System Security Symposium (NDSS)	https://www.ndss-symposium.org
6	International Conference on Theory and Applications of Cryptographic Techniques (EUROCRYPT)	https://eurocrypt.iacr.org
7	International Conference on The Theory and Application of Cryptology and Information Security (ASIACRYPT)	https://asiacrypt.iacr.org/2024/
8	International Conference on Financial Cryptography and Data Security (FC)	https://fc24.ifca.ai/
9	ACM Symposium on Information, Computer and Communications Security (ASIACCS)	https://asiaccs2024.sutd.edu.sg/
10	Workshop on Cryptographic Hardware and Embedded Systems (CHES)	https://ches.iacr.org
20	Simpósio Brasileiro de Cibersegurança (SBSeg)	https://sbseg2024.ita.br/

Preparação dos dados: Os dados usados no levantamento da visão de futuro são *strings* e, portanto, variam em padrões de escrita. A uniformização dos padrões exigiu inicialmente um trabalho manual para conversão dos termos segundo dicionário de palavras-chave. As alterações se deram na uniformização de termos que podem aparecer tanto como siglas quanto por extenso, que podem aparecer com contração etc. Além disso, as *stopwords* foram eliminadas da base, com auxílio de uma biblioteca específica do Python, a *Natural Language Toolkit* (NLTK)[2]. Às *stopwords* foram adicionadas palavras frequentes que não ajudam na identificação de tendências em cibersegurança dada a sua generalização. Por fim, houve ainda uniformização do uso de hífen e decisão sobre o uso de palavras individuais ou expressões compostas. A Tabela 2 lista as *stopwords* acrescentadas, enquanto a Tabela 3 apresenta o dicionário contendo as conversões de palavras realizadas.

Tabela 2: *Stopwords* adicionadas.

***Stopwords* adicionadas**
security
applied
systems
computation
attacks
network
protocols

Análise dos dados e das tendências: Os resultados da análise dos dados e das tendências oferecem o embasamento necessários para a definição dos horizontes de visão de futuro em cibersegurança. A partir da base de dados criada, a ideia é identificar as palavras-chave usadas como nomes de sessões técnicas das principais conferências da área ou como parte dos títulos dos trabalhos publicados na janela de tempo definida. Para isso, nuvens de palavras são usadas para revelar as principais tendências e a sua variação ao longo do tempo. Um outro esforço realizado é a

[2]Disponível em https://www.nltk.org/.

Tabela 3: Dicionário.

Formato original	Formato na base de dados
MPC, Multiparty Computation	Multi-party Computation
ZKP	Zero-Knowledge Proof
Crypto	Cryptography ou Cryptographic (dependendo do contexto)
Cryptocurrency	Cryptographic currency
Priv & Anon	Privacy and Anonymization
PQC, Post quantum	Post-quantum
CPS	Cyber-Physical Systems
Block chain	Blockchain
SCA, Side Channel	Side-channel

contagem do número de aparições das palavras encontradas nos nomes das sessões técnicas ao longo do período analisado.

Identificação de horizontes e mapeamento dos temas: A análise dos dados e das tendências mostram temas relacionados. A ideia desta etapa é revelar tendências, que podem estar mascaradas pelos temas de maior popularidade atual. Para isso, os títulos dos artigos publicados nas conferências selecionadas para a base de dados são usados como entrada de técnicas como *Latent Dirichlet Allocation* e *Inverse Document Frequency*.

3 Análise dos Dados e das Tendências

Esta seção apresenta os resultados obtidos nas etapas de “análise dos dados e das tendências”, que foram usados como subsídios para os resultados da etapa de “identificação de horizontes e mapeamento dos temas”.

Sessões das top conferências no período de 2020 até 2024. Para cada um dos anos considerados na análise, foi gerada uma nuvem de palavras. As Figuras 2, 3, 4, 5 e 6 mostram a nuvem de palavras gerada para 2020, 2021, 2022, 2023 e 2024, respectivamente.

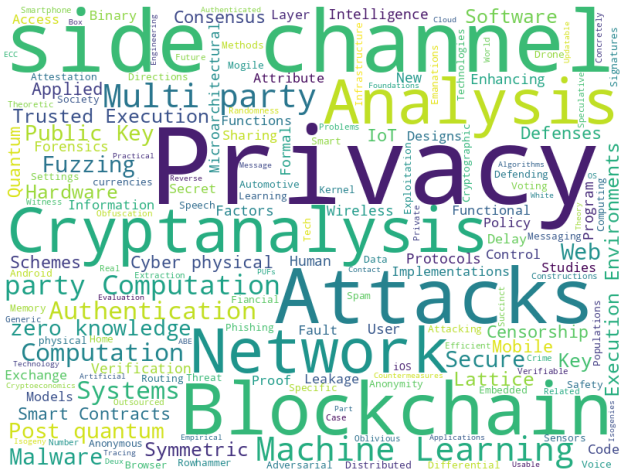


Figura 2: A nuvem de palavras considerando os nomes das sessões técnicas das top-10 conferências internacionais de cibersegurança em 2020.

Pode-se verificar que alguns temas são frequentes, seja pela natureza das conferências, por exemplo, criptografia e privacidade, ou pela perenidade do interesse pelo assunto, como *fuzzing*, *blockchain* e *multi-party computation*.

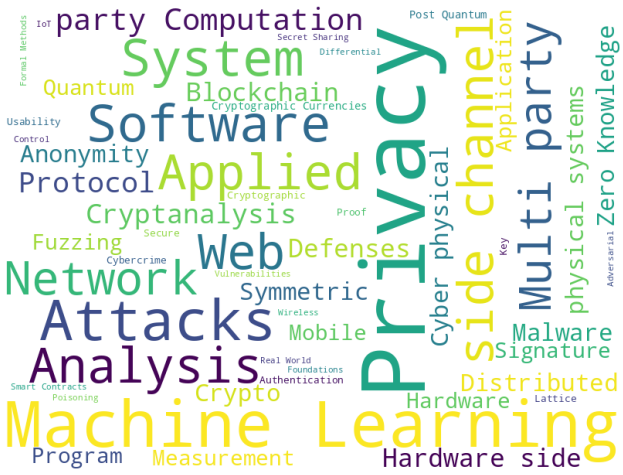


Figura 3: A nuvem de palavras considerando os nomes das sessões técnicas das top-10 conferências internacionais de cibersegurança em 2021.

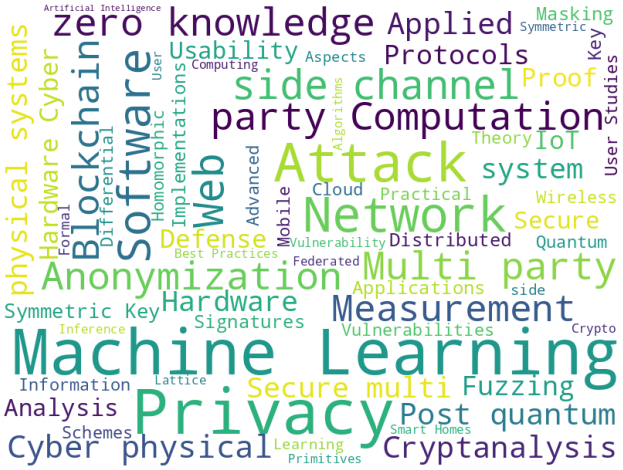


Figura 4: A nuvem de palavras considerando os nomes das sessões técnicas das top-10 conferências internacionais de cibersegurança em 2022.

Figura 5: A nuvem de palavras considerando os nomes das sessões técnicas das top-10 conferências internacionais de cibersegurança em 2023.

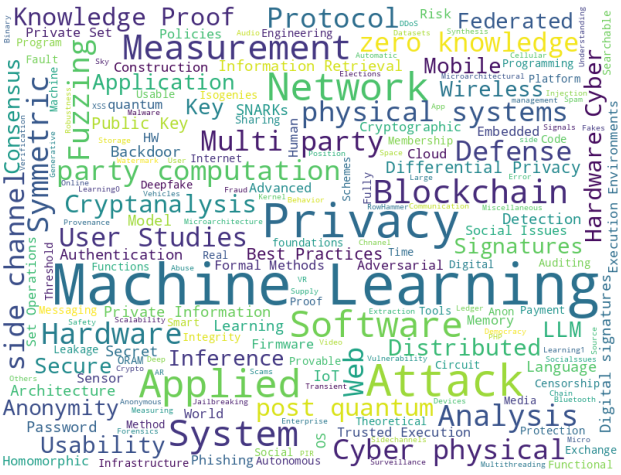


Figura 6: A nuvem de palavras considerando os nomes das sessões técnicas das top-10 conferências internacionais de cibersegurança em 2024.

Alguns temas tornam-se temporariamente esgotados ou de difícil publicação, como é o caso de *malware* e alguns tópicos relacionados a formalismos e fundamentos da segurança, enquanto que outros crescem devido a sua adoção maciça, como é o caso de aprendizado de máquina, ou à questões de inclusão, como é o caso de medições diversas e usabilidade.

Foram geradas também as nuvens de palavras separadas para as top-5 conferências de cada uma das trilhas principais de submissão do SBSeg: Segurança de Sistemas Computacionais e de Redes de Comunicação e Criptografia. As nuvens são apresentadas nas Figuras 7, 8, 9, 10 e 11.

(a) Segurança de Sistemas Computacionais. (b) Criptografia.

Figura 7: Nuvens separadas pelo top-5 de cada área (2020).

A observação das nuvens corrobora as tendências dos tópicos apresentadas nas nuvens gerais, porém permite que se tenha uma visão melhor das conferências de criptografia. Nestas, é evidente a perenidade da área de criptanálise e computação multiparte, aumento no interesse por criptografia simétrica e assinaturas, e diminuição de frequência em criptografia homomórfica e reticulados (*lattice*). Além disso, no último ano, o termo *zero knowledge* não apareceu em destaque, mas sim um tipo especializado dessa prova: *SNARK*, ou *Succinct Non-interactive Argument of Knowledge*.

A Figura 12 representa o número de aparições nos títulos das sessões técnicas das dez palavras mais populares por ano entre 2020 e 2024. Assim, verifica-se a variação da popularidade das palavras ao longo do período analisado. Nota-se que as palavras “machine”, “learning”, “criptography” e “privacy” são as que mais apareceram em título de sessões técnicas desde 2020 e o número de aparições destas palavras está crescendo ano a ano.

(a) Segurança de Sistemas Computacionais. (b) Criptografia.

Figura 8: Nuvens separadas pelo top 5-de cada área (2021).

(a) Segurança de Sistemas Computacionais. (b) Criptografia.

Figura 9: Nuvens separadas pelo top-5 de cada área (2022).

(a) Segurança de Sistemas Computacionais. (b) Criptografia.

Figura 10: Nuvens separadas pelo top-5 de cada área (2023).

(a) Segurança de Sistemas Computacionais. (b) Criptografia.

Figura 11: Nuvens separadas pelo top-5 de cada área (2024).

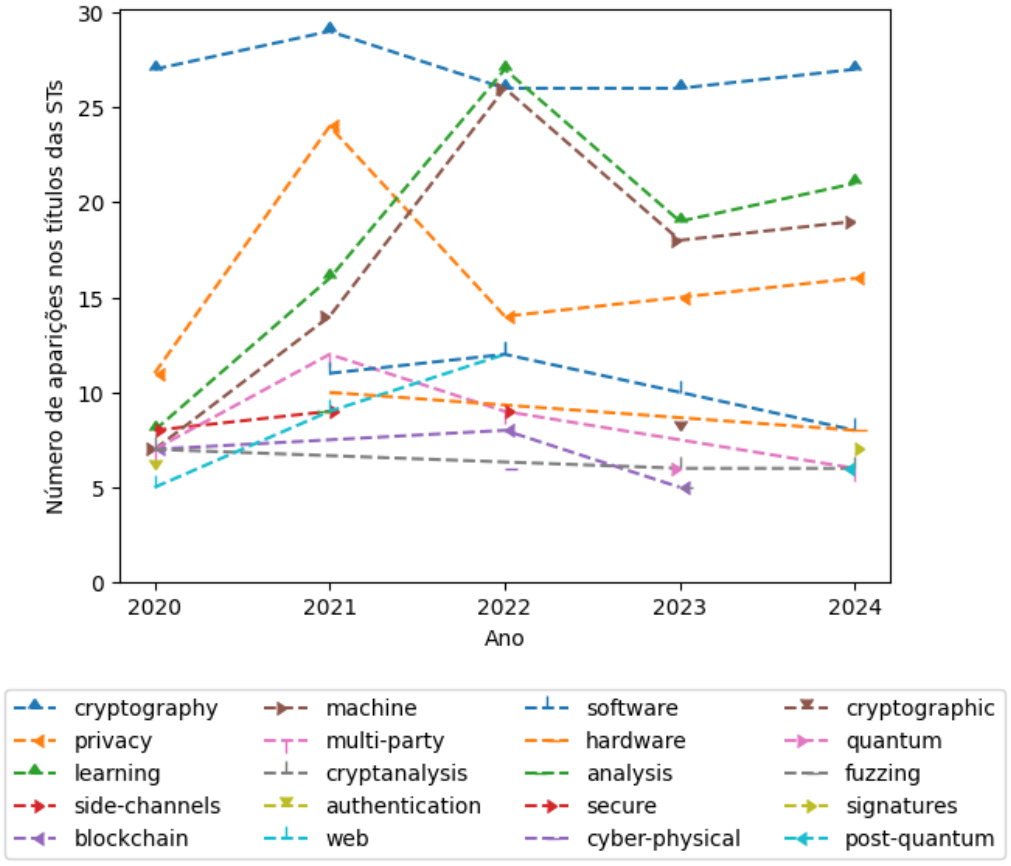


Figura 12: Variação da popularidade das palavras de 2020 a 2024. Toma-se as dez palavras mais populares nos títulos das sessões técnicas por ano para verificar a variação de cada palavra.

Para melhor analisar o impacto do aumento na quantidade de sessões das conferências utilizadas neste documento em relação ao interesse por determinados tópicos, foram selecionados os 15 termos mais frequentes nos títulos das sessões técnicas em 2020 e observou-se sua evolução em um gráfico de fluxo, mostrado na Figura 13.

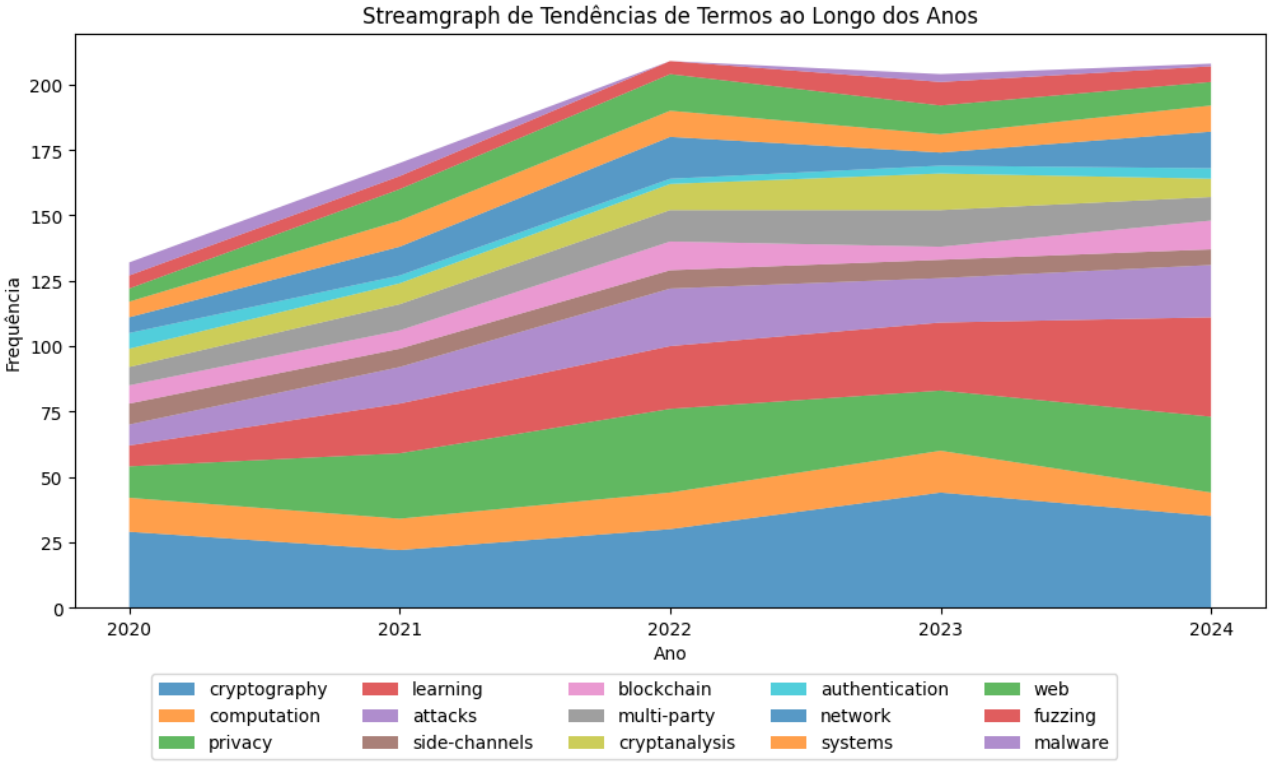


Figura 13: Seleção dos 15 termos mais frequentes nos títulos das sessões técnicas em 2020 e a evolução destes 15 termos de 2020 a 2024.

É possível observar pelo Eixo Y (Frequência) que a ocorrência dos termos cresceu 70% (de aproximadamente 125 para 200), indicando o aumento da quantidade de sessões envolvendo esses termos. Entretanto, ao se analisar cada fluxo individualmente, é possível ver que alguns tópicos se mantiveram estáveis, como é o caso de criptografia, *blockchain*, *multi party computation*, sistemas e Web, enquanto que pós-*quantum*, *malware* e autenticação diminuíram ao ponto de quase não aparecer. Por outro lado, nota-se claramente o aumento de sessões relacionadas à privacidade, devido a questões de evitar censura e proteger vulneráveis, que ficaram mais evidentes recentemente. O maior crescimento, entretanto, é relacionado à *learning*, que aqui pode ser *machine* ou *deep*. Isto mostra que os avanços da área de inteligência artificial e dos *frameworks* que facilitam sua adoção fizeram com que boa parte da pesquisa em cibersegurança migrasse para focar em aplicações de técnicas de aprendizado de máquina em dados de segurança.

Independente do número de sessões por conferência, os resultado obtidos acerca das áreas com redução de interesse, com interesse constante, ou com aumento de interesse entre 2020 e 2024 são corroborados pelo mapa de calor temporal da Figura 14, cujos dados de entrada referentes à frequência de aparição dos 15 termos mais populares em 2020 foram normalizados.

A Tabela 4 apresenta a quantidade de sessões por conferência dentre as selecionadas ao longo do período investigado. Os dados mostram que o Usenix Security Symposium mais do que triplicou de tamanho durante o período. Outras conferências praticamente dobraram de tamanho de 2020 para 2024, como ACM CCS, CRYPTO, NDSS, EUROCRYPT, ASIACRYPT. Já o IEEE S&P, a FC, ASIACCS e CHES não apresentaram crescimento considerável de tamanho (sessões e, consequentemente, aceitação de artigos).

Identificação de horizontes e mapeamento dos temas

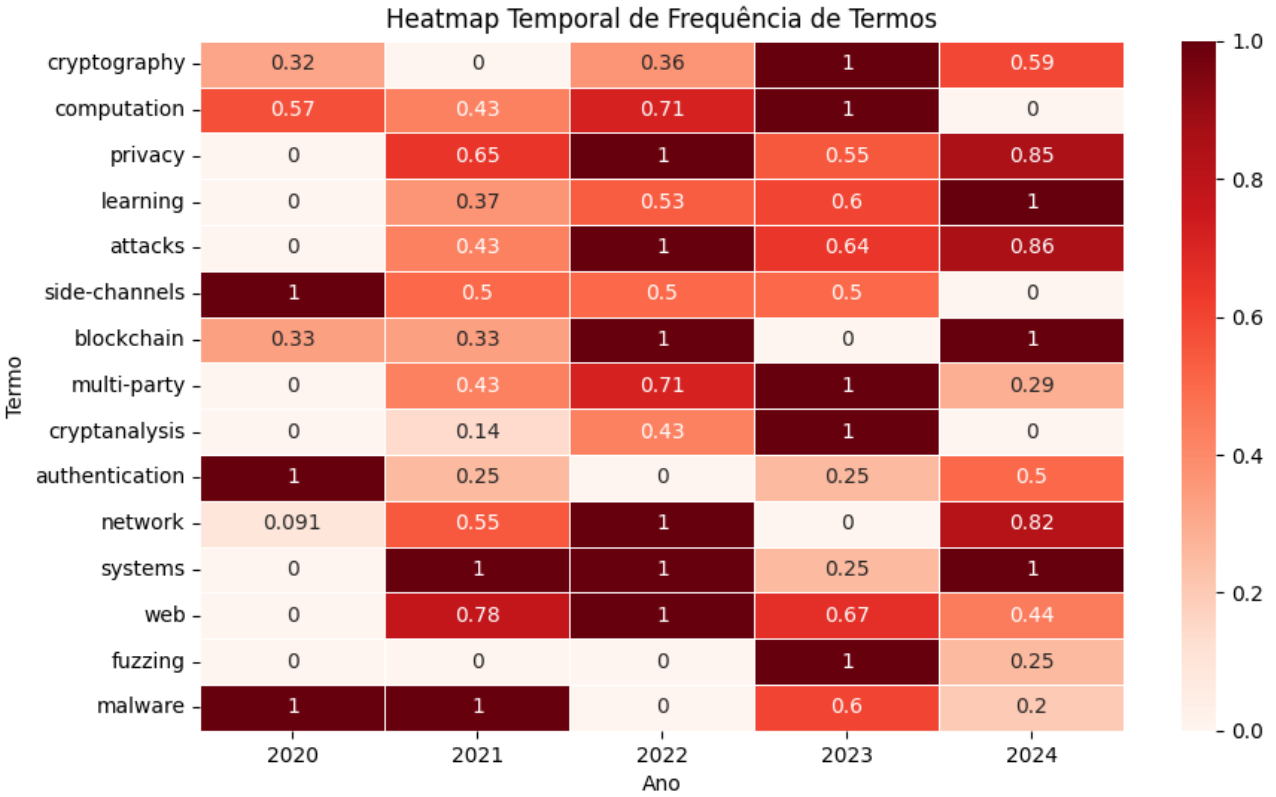


Figura 14: Mapa de calor normalizado dos 15 termos mais frequentes em 2020 e a evolução destes 15 termos entre 2020 e 2024.

Tabela 4: Quantidade anual de sessões por conferência entre 2020 e 2024.

Conferência	**2020**	**2021**	**2022**	**2023**	**2024**
ACM CCS	33	40	65	59	61
IEEE S&P	26	39	36	35	36
Usenix Security	29	36	60	90	98
CRYPTO	15	25	28	57	39
NDSS	22	21	21	23	39
EUROCRYPT	14	13	30	43	33
ASIACRYPT	19	16	28	29	N/D
FC	10	12	11	10	12
ASIACCS	16	18	18	18	21
CHES	12	13	12	15	12

As análises anteriores mostraram que temas relacionados a aprendizado de máquina têm crescido, mas por serem baseadas na maior frequência dos termos, não permitem a identificação de novos tópicos que estão para se popularizar.

Com o objetivo de observar tópicos que podem se tornar tendência de publicações, foram analisados os títulos dos artigos aceitos para publicação nas conferências selecionadas neste documento, para os quais aplicou-se a técnica *Latent Dirichlet Allocation* (LDA), que é utilizada em processamento de linguagem natural para extrair tópicos e palavras-chave em texto (ZIMMERMANN et al., 2024). Foram obtidos os títulos dos artigos das conferências selecionadas, os quais serviram de entrada para a técnica LDA, com valor dos argumentos de entrada “tópicos” e “palavras-chave” igual a 10 e 3, respectivamente, ou seja, dez tópicos mais relevantes e três palavras-chaves que os representem.

- **ACM CCS**
  1. fuzzing, efficient, memory
  2. private, inference, model
  3. attack, proofs, towards
  4. models, language, attack
  5. authentication, information, retrieval
  6. training, trees, qualitative
  7. privacy, learning, secure
  8. attack, privacy, schemes
  9. detection, attack, detecting
  10. secure, data, computation
- **IEEE S&P**
  1. data, learning, model
  2. learning, backdoor, attacks
  3. fuzzing, devices, large
  4. graph, efficient, models
  5. vulnerabilities, towards, understanding
  6. scalable, distributed, practical
  7. adversarial, framework, attacks
  8. privacy, differential, attack
  9. attacks, models, practical
  10. analysis, detection, efficient
- **USENIX Security**
  1. machine, learning, oblivious
  2. privacy, scale, behavior
  3. go, adversarial, reality
  4. attack, efficient, models
  5. attack, data, user
  6. protecting, users, mitigation
  7. web, fuzzing, code

8. model, data, detection
9. privacy, attack, learning
10. state, data, testing

- **CRYPTO**

1. codes, efficient, signatures
2. commitments, lwe, lattices
3. signatures, assumptions, proofs
4. cryptography, functions, quantum
5. improved, key, exchange
6. fhe, cryptanalysis, distributed
7. zero, knowledge, generic
8. attacks, algebraic, computation
9. quantum, encryption, threshold
10. secret, sharing, computation

- **NDSS**

1. attack, enhancing, analysis
2. models, leveraging, blockchain
3. privacy, protocol, networks
4. attack, detection, data
5. model, attestation, deep
6. authentication, linux, kernel
7. computation, efficient, secure
8. attack, adversarial, recognition
9. vulnerabilities, smart, ethereum
10. authentication, fuzzing, privacy

- **EUROCRYPT**

1. efficient, tweakable, pir
2. framework, attacks, lpn
3. arithmetic, circuits, consensus
4. threshold, output, practical
5. random, certified, assumptions
6. encryption, functional, bootstrapping
7. new, signatures, complexity
8. circuits, optimal, differential
9. secret, sharing, homomorphic
10. key, tight, attacks

- **ASIACRYPT**

1. signatures, threshold, unforgeability

2. applications, threshold, cryptanalysis
3. proofs, bootstrapping, model
4. computation, revisiting, key
5. linear, communication, structure
6. key, generic, signatures
7. private, set, analysis
8. efficient, secure, problem
9. quantum, key, new
10. encryption, functional, registered

- **FC**

1. decentralized, market, making
2. attacks, cryptographic, blockchain
3. blockchain, key, decentralization
4. attacks, cryptographic, blockchain
5. optimal, fees, blockchain
6. signatures, anonymous, attacks
7. power, accountable, fees
8. latency, consensus, cryptographic
9. short, paper, attacks
10. verifiable, decentralization, short

- **ASIACCS**

1. analysis, command, protection
2. iot, web, model
3. privacy, analysis, framework
4. based, anonymous, edge
5. memory, automated, cache
6. execution, trusted, environments
7. efficient, secure, public
8. key, formal, communication
9. attacks, networks, payment
10. learning, fuzzing, targeted

- **CHES**

1. attacks, application, physical
2. masked, implementation, signatures
3. homomorphic, evaluation, secure
4. analysis, circuits, noise
5. faster, bootstrapping, cryptography
6. power, analysis, attacks
7. leakage, probing, encryption

8. efficient, keccak, framework
9. masking, attacks, optimized
10. hardware, masking, fault

- **SBSeg**

1. contra, impacto, anomalias
2. detecção, explicável, inteligência
3. malware, detecção, android
4. detecção, ataques, cryptographic
5. classificação, models, vulnerabilidades
6. análise, detecção, software
7. learning, algorithms, rede
8. estratégias, rede, detecção
9. detection, dispositivos, attack
10. redes, explicável, dados

É possível notar uma tendência voltada para a pesquisa em ataques adversariais contra modelos de aprendizado de máquina, criptografia diferencial/homomórfica e eficiência, além de *fuzzing* em alvos diversos ser um tema constante.

Ao se analisar as palavras-chaves dos artigos aceitos para a conferência IEEE Security & Privacy 2024 (Figura 15), cujos meta-dados estão disponíveis para *download* em https://developer.ieee.org/, percebe-se alguns termos que começaram a aparecer e podem indicar a tendência para o estado da arte.

Figura 15: A nuvem de palavras feita a partir das palavras-chaves dos artigos aceitos em 2024 pela conferência IEEE Security & Privacy.

Nota-se termos como *Voting* (de votação eletrônica), *Voice* (relacionado à pesquisas de autenticação, *speech to text* ou *deep fake*), *waste* e *water* (relacionado com sustentabilidade, que se tornou uma preocupação geral, incluindo pegada de carbono gerada por uso maciço de GPUs) e *Transformers* (que ficaram populares para diversas aplicações de *chatbots* ou como parte de detectores/classificadores multi-modais).

A Figura 16 mostra a nuvem de palavras referente aos títulos dos artigos publicados no SBSeg desde sua primeira edição, em 2001, até a mais recente, em 2024. Além de utilizar o conjunto padrão de *stopwords* em português, foram adicionadas as palavras 'segurança', 'baseado', 'baseada', 'mecanismo', 'método' e 'sistema', a fim de remover ruído que prejudicasse a interpretação do gráfico gerado. É possível observar entre as palavras mais frequentes: detecção, rede, ataque, análise, controle, arquitetura, dados, avaliação, modelo, acesso, intrusão, vulnerabilidade, aprendizado, usuário e *malware*, dando indícios dos tópicos de maior apelo ao longo da existência do evento.

Figura 16: A nuvem de palavras feita a partir dos títulos de artigos publicados no SBSeg de 2001 a 2024.

A Figura 17 mostra as palavras frequentes escolhidas na submissão de artigos para o SBSeg 2023. É possível notar que *machine learning* domina os tópicos de submissão. Ao se analisar os artigos efetivamente publicados, nota-se grande quantidade de trabalhos relacionados à aplicações de *machine learning* em algum domínio da segurança. Outros termos, como *malware* e *intrusion detection* são ligados em sua maioria a artigos que dependem de aprendizado de máquina para obter resultados de suas propostas.

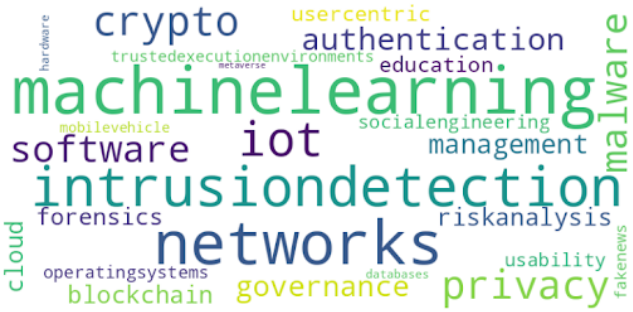


Figura 17: A nuvem de palavras feita a partir dos tópicos das submissões do SBSeg 2023.

A Figura 18 mostra que, em geral, os temas dos artigos nacionais são constantes ao longo dos anos. Ao comparar-se as Figura 18 e 16, o que chama a atenção são as palavras “ransomware” e “Android”, pois são tópicos mais atuais e, consequentemente, não existiam ou eram incomuns nas edições mais antigas do evento.

4 Panorama Nacional

A relevância do tema cibersegurança tem aumentado no país. Do ponto de vista estratégico e legal, o marco no horizonte analisado entre 2020 e 2024 inicia com a Estratégia Nacional de Segurança Cibernética (E-Ciber) de 2020 que estabeleceu diretrizes e metas para fortalecer a cibersegurança no Brasil e culminando com o Decreto nº 11.856, de 26 de dezembro de 2023 que institui a Política Nacional de Cibersegurança (PNCiber) e cria o Comitê Nacional de Cibersegurança (CNCiber), o país passa a ter diretrizes e metas para orientar a cibersegurança. Atualmente, a revisão da E-Ciber encontra-se em andamento CNCiber por meio de um Grupo de Trabalho Temático criado para tal finalidade e a RNP tem uma vaga no CNCiber como representante das instituições científicas,

Figura 18: A nuvem de palavras feita a partir dos títulos dos artigos aceitos para publicação no SBSeg 2024.

tecnológicas e de inovação relacionadas à área de cibersegurança. Ainda considerando a questão regulatória, as agências reguladores (ANPD, ANEEL, ANATEL, ANA e ANVISA) tem se preocupado com o tema, tendo cada uma delas regulamentado os aspectos de cibersegurança específicos das áreas em que atuam. Apesar de todos esse esforços, conforme apontado em relatório do Tribunal de Contas da União (TCU) o país ainda não conta com uma entidade com capacidade de guiar as ações e políticas nacionais em cibersegurança e esse é desafio para os próximos anos (TRIBUNAL DE CONTAS DA UNIÃO, 2024).

Outras entidades também têm realizado ações relacionadas à cibersegurança tendo o exemplo mais recente o programa Hackers do Bem, coordenado e executado pela RNP e pelo SENAI-SP, e outros programas de formação profissional na área, a realização do exercícios Guardião Cibernético pelas forças armadas brasileiras, e eventos diversos para discussões técnicas sobre o tema.

Quando se considera a pesquisa e inovação, observando por exemplo os grupos de pesquisa registrados no CNPq, observa-se que 49 grupos de pesquisa com produção na área, estando geograficamente distribuídos conforme a Figura 19. Esse grupos tem pesquisado sobre temas como criptografia, detecção de intrusão, *ransomware*, até aplicações de IA em cibersegurança, sendo este último tema uma tendência nas produções mais recentes.

Quando se observa a produção nacional de dissertações e teses na área, considerando a bases de dados da CAPES, ao analisar os temas mais tratados nos resumos observa-se uma grande variedade, tendo “segurança da informação” como o mais encontrado, porém com tendência de surgimento de outros temas voltas à camada física, como Internet das Coisas e Tecnologia Operacional e a aplicação de Inteligência Artificial, como representado na Figura 20 que tem a sequência de palavras mais citadas nos últimos três anos.

A análise dos dados do INPI por patentes e registros de software considerando os termos relacionas à Cibersegurança demonstra poucas atividades. Não foram encontrados registros de software, e somente 5 (cinco) patentes.

Um movimento recente no país são iniciativas para criação de centros especializados em temas estratégicos. Em cibersegurança, foram criados ao menos dois centros de competência, sendo um por iniciativa da FAPESP no estado de São Paulo e outro por iniciativa de Embprapii que está localizado em Recife-PE. Outra entidade não diretamente dedicada ao tema, mas que será capaz de produzir resultados importantes para a cibersegurança no país é o Centro de Competência em Tecnologias Quânticas no SENAI-CIMATEC em Salvador-BA.

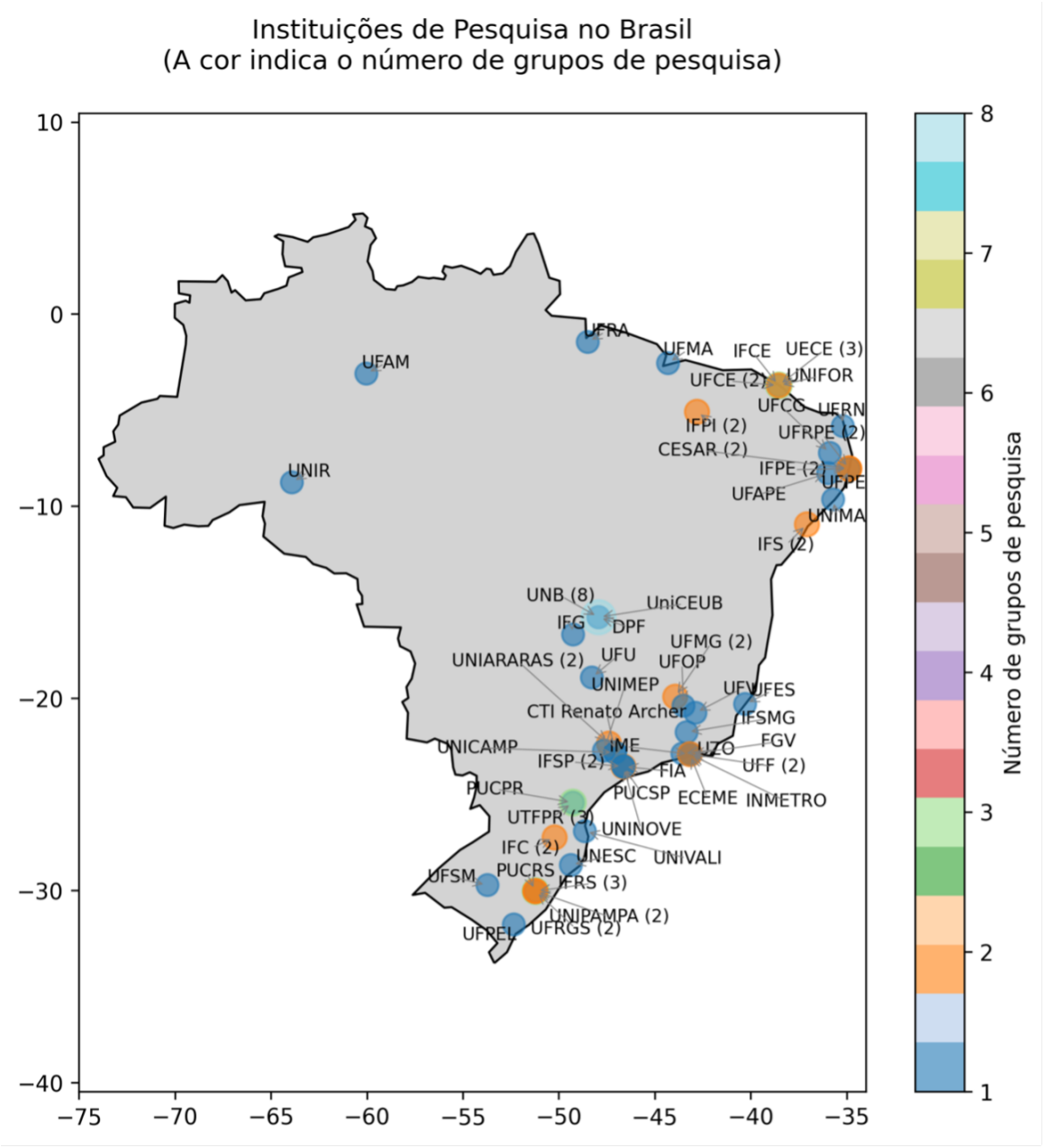
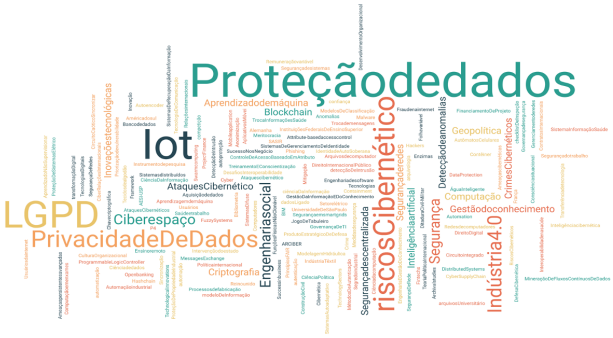


Figura 19: Distribuição geográfica dos grupos de pesquisa CNPq com linha de pesquisa ativa em cibersegurança.



(a) 2022. (b) 2023.

(c) 2024.

Figura 20: Termos mais citados nos resumos das dissertações e teses disponíveis nas bases de dados da CAPES de acordo com o ano.

4.1 Tendências das Iniciativas Nacionais

Conforme apresentado na Seção 4, o tema de cibersegurança no Brasil tem sido analisado sob os mais diversos aspectos e níveis de profundidade. Entretanto, nota-se que alguns pontos tem recebido mais atenção:

1. **Governança e Proteção de Dados:** com as regulações estabelecidas o país passou ao contar com entidades nacionais que tratam exclusivamente da cibersegurança. Como exemplo, nota-se a crescente atuação da ANPD e do CNCiber que têm avançado na regulamentação e na governança da cibersegurança no país. Porém, há ainda muito o que se avançar e, preferencialmente, em pouco anos.
2. **Temas de Pesquisa:** nota-se que a pulverização de temas associados à cibersegurança, porém nos últimos anos há indícios do direcionamento das pesquisas para a segurança em Internet das Coisas, redes de comunicações móveis e utilização da inteligência artificial em cibersegurança. Sejam nos temas de dissertação e teses, ou chamadas por agências de fomento, começa a despontar o interesse pelas tecnologias quânticas ou relacionados como a criptografia pós-quântica.
3. **Iniciativas:** observa-se que há um conjunto de iniciativas nacionais pela criação de centros de competências em cibersegurança e outras relacionadas à tecnologias quânticas que terão impacto na área de cibersegurança em um futuro próximo.

Embora haja avanços, foi observado que há espaço para melhorias como a criação de uma entidade nacional de cibersegurança para guiar as ações no tema, podendo inclusive indicar tema prioritários de pesquisa e desenvolvimento na área. A quantidade de registro de software ou de patentes no INPI é baixa. Embora com os dados levantados não seja possível precisar o motivo, este pode ser uma tendência que necessite de atenção para que seja alterada.

5 Panorama Internacional

A cibersegurança surge como uma área crítica na pesquisa internacional, impulsionada pela crescente complexidade dos ecossistemas digitais e pela natureza evolutiva das ciberameaças. Uma análise das principais iniciativas de pesquisa nos Estados Unidos e na Europa destaca as principais tendências e possíveis direções para investigações futuras. O cenário de pesquisa explora tópicos avançados, como criptografia quântica, estruturas de segurança adaptáveis orientadas à Inteligência Artificial e a conformação regulatória transfronteiriça. No Brasil, a crescente adoção de plataformas digitais e iniciativas como a E-Ciber se alinham às tendências globais, com foco na proteção de infraestrutura crítica, privacidade de dados e desenvolvimento da força de trabalho em cibersegurança. Esses paralelos sugerem que a pesquisa brasileira pode integrar percepções de esforços internacionais para abordar desafios regionais únicos, ao mesmo tempo em que contribui para avanços globais.

As descobertas apresentadas nesse relatório são derivadas de uma metodologia detalhada envolvendo análise orientada por dados. Projetos dos EUA financiados pela NSF (*National Science Foundation*) sob a diretoria CISE (*Computer and Information Science and Engineering*), iniciados a partir de 2019, foram selecionados com base em seu foco em cibersegurança, conforme indicado em seus títulos ou resumos. Projetos europeus foram identificados como aqueles financiados pela Comissão Europeia desde 2021. Os projetos europeus selecionados são os que têm a palavra-chave "*cybersecurity*". A análise seguiu estas etapas:

- **Processamento de dados**: projetos que atendem aos critérios especificados foram filtrados;

- **Seleção de projetos**: apenas projetos CISE iniciados a partir de 2019 e projetos europeus iniciados após 2021, com *cybersecurity* como palavra-chave, foram incluídos;
- **Extração temática**: foi utilizada a metodologia descrita na Seção 2, usando PLN e o modelo de LDA, os projetos foram categorizados em temas distintos com base em tópicos em seus títulos e resumos.

Essa abordagem estruturada garante uma visão abrangente das prioridades de pesquisa em evolução em cibersegurança nessas regiões.

5.1 Investimentos em Áreas Críticas de Cibersegurança

O Plano Estratégico de Cibersegurança da CISA (Cybersecurity and Infrastructure Security Agency) para o triênio 2024-2026 enumera as áreas mais críticas de investimento nos Estados Unidos, enfatizando a colaboração e a resposta estratégica às ameaças em evolução (CISA, 2024). As principais áreas críticas de investimento em cibersegurança no panorama internacional são enumeradas a seguir.

1. **Inteligência Artificial e Aprendizado de Máquina (IA/ML)**: Nos Estados Unidos, projetos financiados pela NSF neste domínio, como “AI-CyS Research Partnership”, receberam mais de US$ 150 milhões coletivamente, com foco na integração de IA para detecção e mitigação preditiva de ameaças. O plano CISA destaca a importância de alavancar a IA para desenvolver ferramentas proativas para detecção de ameaças em tempo real e automação de resposta, alinhando-se com prioridades nacionais mais amplas. Na Europa, iniciativas impulsionadas por IA como o projeto “KARTOS” receberam aproximadamente €75 milhões, enfatizando o gerenciamento de risco e a análise de cibersegurança com tecnologias de IA.
2. **Cibersegurança em tecnologias emergentes**: Os EUA direcionaram mais de US$ 100 milhões para proteger tecnologias emergentes, como visto em iniciativas como no projeto “Cybersecurity for Smart Manufacturing”. A estratégia do plano da CISA enfatiza a proteção de tecnologias modernas, como IA e computação quântica, que são cada vez mais críticas para a resiliência nacional e industrial. O projeto europeu “HORSE” e iniciativas semelhantes receberam perto de € 50 milhões, visando ecossistemas 6G seguros e princípios de rede sustentáveis.
3. **Abordagens centradas na comunidade e baseadas em dados**: Os investimentos nos EUA, como no projeto “CCRI: New Data-Driven Cybersecurity Research Infrastructure”, ultrapassam US$ 200 milhões, com foco em plataformas colaborativas para setores críticos. O foco da CISA na construção de mecanismos de defesa robustos por meio de parcerias comunitárias e compartilhamento aprimorado de inteligência de ameaças destaca objetivos paralelos. Esforços europeus como o projeto “EasyDC-FOS” foram apoiados com cerca de € 60 milhões para aprimorar infraestruturas de compartilhamento de dados e soluções baseadas na comunidade.
4. **Abordagens dos impactos sociais da cibersegurança**: O projeto dos EUA sobre detecção precoce de ameaças com base em mídia social foi financiado com US$ 100 milhões, abordando desinformação e resiliência social. O plano CISA ressalta a urgência de abordar vulnerabilidades críticas nos setores público e privado, incluindo a melhoria da higiene cibernética de cidadãos e empresas. Na Europa, projetos como o “HAL4SDV” receberam mais de € 70 milhões, abordando a cibersegurança em veículos definidos por software e sistemas sociais críticos.
5. **Estruturas políticas e legislativas**: Iniciativas políticas europeias como a Diretiva NIS2 e a Lei de Resiliência Cibernética são apoiadas por amplo financiamento por meio de mecanismos nacionais e da UE, excedendo coletivamente a € 500 milhões. Esses investimentos se concentram em aumentar a resiliência em setores-chave, como energia, saúde e infraestrutura digital.

A estratégia CISA e o relatório sobre o estado da cibersegurança na União Europeia destacam o fortalecimento das políticas de cibersegurança e relatórios de incidentes como pilares fundamentais, alinhando-se com os avanços legislativos globais. O investimento financeiro significativo ressalta a importância atribuída à pesquisa de cibersegurança globalmente e destaca áreas de oportunidade para mais avanços e colaborações.

5.2 Tendências das Iniciativas Internacionais

A cibersegurança evolui como um campo dinâmico e multidisciplinar, refletindo a crescente dependência de sistemas digitais e a sofisticação das ameaças *online*. Esta seção se aprofunda nas últimas tendências que moldam a pesquisa de cibersegurança nos Estados Unidos e na Europa. Ao examinar os principais projetos e iniciativas, destaca-se como os desafios emergentes são abordados no cenário internacional e capitalizam os avanços tecnológicos. Esses esforços não apenas aumentam a resiliência contra ciberameaças, mas também preparam o cenário para inovação colaborativa e desenvolvimento de políticas no cenário global de cibersegurança.

1. Inteligência Artificial e Aprendizado de Máquina (IA/ML): Tanto nos Estados Unidos quanto na Europa, alavancar IA e ML para aprimorar os recursos de cibersegurança é uma tendência proeminente;
2. Cibersegurança em tecnologias emergentes: A pesquisa abordando as vulnerabilidades em tecnologias emergentes está crescendo. A iniciativa dos EUA e na Europa exploram a proteção de sistemas de manufatura interconectados e de novas tecnologias de comunicação como 5G e 6G, por meio de soluções orientadas por IA;
3. Abordagens baseadas em dados e centradas na comunidade: ambas as regiões enfatizam estruturas de compartilhamento de dados e plataformas de pesquisa colaborativa;
4. Abordagens dos impactos sociais da cibersegurança: As implicações sociais das violações de cibersegurança, como tecnologia de *deepfake* e desinformação, estão ganhando atenção;
5. Estruturas Políticas e Legislativas: A Europa fez avanços significativos na criação e conformação de políticas de cibersegurança por meio de iniciativas como a Diretiva NIS2 e a Lei de Resiliência Cibernética (CRA). Essas estruturas visam melhorar as capacidades de preparação e resposta em níveis nacional e da UE, abordando vulnerabilidades em setores críticos como energia, saúde e infraestrutura digital. O relatório ENISA 2024 destaca a importância de uma legislação abrangente para lidar com a segurança da cadeia de suprimentos, ransomware e ameaças híbridas avançadas.

As tendências do cenário de pesquisa abordam desafios e oportunidades emergentes apresentados pela evolução tecnológica e pela interconectividade global. Essas direções destacam potenciais avanços e áreas de foco que moldarão o futuro da resiliência digital em todo o mundo. Ao antecipar a próxima onda de inovações e ameaças, pesquisadores e formuladores de políticas podem alinhar esforços para proteger sistemas e infraestruturas críticas, garantindo que os ecossistemas digitais globais permaneçam seguros e sustentáveis. Algumas tendências identificadas em projetos de pesquisa internacionais são:

1. **Criptografia pós-quântica**: À medida que a computação quântica avança, garantir a resiliência criptográfica contra ataques quânticos se tornará uma prioridade. Espera-se que os investimentos em criptografia pós-quântica e padrões relacionados cresçam significativamente.
2. **Cibersegurança em sistemas autônomos**: A ascensão de sistemas autônomos, incluindo veículos e *drones*, exige mecanismos de segurança robustos. A pesquisa se concentrará em

proteger protocolos de comunicação, prevenir sequestro de sistemas e garantir a integridade dos dados.

3. **Segurança integrada para sistemas multidomínio**: Com a convergência de TI e tecnologia operacional (OT), proteger ambientes multidomínio se tornará crítico. Isso inclui soluções intersetoriais que abordam vulnerabilidades em saúde, manufatura e cidades inteligentes, por exemplo.

4. **IA ética e governança**: À medida que os sistemas de IA desempenham um papel maior na cibersegurança, considerações éticas e estruturas de governança ganharão destaque. A pesquisa abordará viés algorítmico, transparência e responsabilidade em ferramentas de cibersegurança orientadas por IA.

5. **Educação em cibersegurança e desenvolvimento da força de trabalho**: A escassez global de profissionais de cibersegurança destaca a necessidade de iniciativas educacionais inovadoras. Programas com foco em grupos sub-representados, como visto na parceria AI-CyS dos EUA, podem servir como modelos para ampliar a participação e a *expertise* em cibersegurança.

6. **Fortalecimento da segurança da cadeia de suprimentos e infraestruturas críticas**: O relatório da European Union Agency for Cybersecurity (ENISA) (ENISA, 2024) ressalta a criticidade de abordar as vulnerabilidades da cadeia de suprimentos, que têm implicações de longo alcance. Abordagens multifacetadas envolvendo avaliações de risco coordenadas em toda a UE e estruturas regulatórias são essenciais para mitigar os efeitos em cascata dos ataques à cadeia de suprimentos.

7. **Gestão de crises e preparação**: O desenvolvimento de estruturas robustas de gestão de crises, conforme enfatizado pela ENISA, será fundamental. Espera-se que investimentos em exercícios de cibersegurança, mecanismos de relatórios de incidentes e respostas coordenadas da UE a incidentes de grande escala aumentem a resiliência de sistemas computacionais.

O cenário de pesquisa internacional em cibersegurança demonstra um forte alinhamento em direção ao enfrentamento de desafios contemporâneos enquanto se prepara para ameaças futuras. Esforços colaborativos, tecnologias inovadoras e iniciativas educacionais inclusivas serão essenciais para aumentar a resiliência global da cibersegurança. Ao promover parcerias interdisciplinares e transfronteiriças, a comunidade de pesquisa pode combater efetivamente o cenário de ciberameaças em constante evolução. Os esforços europeus, particularmente por meio de avanços legislativos e políticos, fornecem um modelo robusto para alinhar estratégias nacionais e regionais para enfrentar os desafios globais de cibersegurança.

6 Visão de futuro em Cibersegurança

As projeções de temas em evidência em cibersegurança estão organizados em três horizontes distintos de tempo: curto (próximos 2 anos), médio (entre 2 e 5 anos), e longo prazo (entre 5 e 10 anos). Esses temas podem nortear novos editais de P,D&I e novas oportunidades de serviços e produtos oferecidos pela RNP às instituições do sistema RNP.

6.1 Primeiro horizonte

Publicações internacionais nas top conferências de cibersegurança começaram a ter como tema em 2024 o uso mais intenso de aprendizado de máquina, principalmente de pesquisa baseada em aplicações de grandes modelos de linguagem (KUCHARAVY et al., 2024). Portanto, este é uma forte tendência para os próximos 2 anos. Conforme as chamadas “máquinas de IA” ficarem mais populares

e seja possível treinar modelos regionalizados do zero (por exemplo, em português), é provável que novas abordagens surjam, seja para auxiliar na tomada de decisões, *chatbots* para educação e conscientização, ou criação de relatórios de análise/inteligência automatizados que expliquem *logs*, tráfego de rede e IoCs (*Indicators of Compromise*) relacionados à análise de ameaças. Atualmente, tem-se feito uso de modelos pré-treinados, com ajustes finos (*fine tuning*) para especializá-los em contextos específicos, como verificação de código-fonte. Essas tecnologias podem servir também para análise de código-fonte criptográfico em busca de vulnerabilidades ou suporte à criptanálise.

CISA e ENISA afirmam em seus relatórios mais recentes (CISA, 2024; ENISA, 2024) que a educação em cibersegurança e o aumento da força de trabalho em cibersegurança são desafios imediatos por conta da escassez global de profissionais capacitados na área. No Brasil, o programa Hackers do Bem é um sucesso, tendo mais de 100 mil inscritos interessados em capacitação gratuita em cibersegurança. O cenário, portanto, é de falta de profissionais, mas, ao mesmo tempo, de muito interesse de pessoas buscando se capacitar. É preciso, então, desenvolver iniciativas para aumentar o número de estudantes em cibersegurança, aumentar o número de cursos em cibersegurança, aumentar o número de organizações e pessoas capazes de fornecer cursos em cibersegurança e desenvolver ferramentas inovadoras para o ensino de cibersegurança, como as fomentadas pela RNP via programa Hackers do Bem e soluções advindas de Grupos de Trabalho, que podem utilizar o próprio ecossistema da RNP como plataforma de experimentação.

Tecnologias de cibersegurança, como SIEM (*Security Information and Event Management*) e EDR (*Endpoint Detection and Response*), já estão consolidadas no mercado e desempenham um papel fundamental nas operações de cibersegurança. Essas soluções possuem alta confiabilidade, amplo suporte e estão bem integradas aos ecossistemas empresariais. Elas oferecem funcionalidades robustas para monitoramento de eventos e respostas rápidas a incidentes, sendo indispensáveis para a manutenção da integridade e da segurança nos ambientes corporativos atuais. Organizações que ainda não adotaram essas tecnologias devem considerá-las prioritárias devido à sua maturidade e impacto comprovado na redução de riscos. As pesquisas nesses temas são incrementais ao amplo conhecimento já disponível e ao grande número de trabalhos publicados. Porém, tanto SIEM e EDR podem ser oferecidos pelo SOC da RNP como serviço para instituições do sistema RNP, inclusive com a chamada de Grupos de Trabalho especializados para atuar nesse tipo de solução.

6.2 Segundo horizonte

Pesquisas em arquiteturas de confiança zero (*Zero Trust*) e Inteligência Artificial Generativa representam a fronteira de inovação para desafios que devem se intensificar em um horizonte de médio prazo, isto é, entre 2 e 5 anos. Esses temas se alinham com projetos internacionais em desenvolvimento, além de iniciativas de grupos nacionais. Os temas convergem na necessidade urgente de garantir segurança, privacidade e interoperabilidade em um cenário digital cada vez mais distribuído, dinâmico e impulsionado por automação inteligente. O modelo de confiança zero responde à crescente sofisticação das ciberameaças e a IA generativa aplicada a ambientes de cibersegurança surge como força disruptiva na tomada de decisão e geração de políticas, exigindo novos mecanismos de controle, explicabilidade e confiança. A IA generativa, por exemplo, relaciona-se com o uso mais intenso de técnicas de aprendizado de máquina (do primeiro horizonte), mas agora podendo ser também aplicada à geração de políticas e automação avançada de soluções de cibersegurança, bem como pode ser usada para gerar IoCs ou automatizar análises de forense digital.

Trabalhos de pesquisa que exploram tecnologias como *Digital Forensics and Incident Response* (DFIR), *Extended Detection and Response* (XDR), *Threat Intelligence Products and Services* e Serviços MDR (*Managed Detection and Response*) têm chance de crescer, uma vez que são evoluções naturais de SIEM/EDR, com foco em integração e resposta proativa. Essas tecnologias estão em fase de amadurecimento e adoção crescente com casos de uso validados. Nesse contexto, empresas podem explorar soluções como o gerenciamento de superfícies de ataque externas e

ferramentas avançadas de detecção e resposta a ameaças para fortalecer sua postura de segurança. Embora essas tecnologias ainda necessitem de integração e ajustes, elas já apresentam valor significativo em ambientes que demandam proteção proativa e inteligência contra ameaças.

6.3 Terceiro horizonte

As tendências do horizonte de longo prazo, entre 5 e 10 anos, incluem criptografia pós-quântica, *Threat Exposure Management*, CAASM (*Cyber Asset Attack Surface Management*), *Cybersecurity AI Assistants* e SOCs quase que totalmente gerenciados por IAs, representando o futuro das operações de cibersegurança. Essas tecnologias estão atualmente no estágio de gatilho de inovação, em que o foco está na experimentação e no desenvolvimento. Por serem promissoras, mas ainda pouco maduras, sua implementação demanda tempo e recursos para superar desafios técnicos e operacionais. Além disso, tecnologias como arquitetura de cibersegurança em malha (*Cybersecurity Mesh Architecture* - CSMA) e mecanismos de Avaliação Automatizada de Controle de Segurança (*Automated Security Control Assessment* - ASCA) têm forte potencial inovador, mas ainda necessitam de mais de uma década para atingir ampla adoção. Organizações interessadas em inovação de longo prazo devem acompanhar o progresso dessas tecnologias, investindo estrategicamente em pilotos e parcerias que acelerem sua maturação. Há grandes possibilidades para desenvolvimento de projetos de P,D&I nesses temas.

Um outro ponto a ser considerado para este horizonte diz respeito aos avanços em *hardware*, os quais podem permitir o desenvolvimento de mecanismos inovadores de proteção que atuem antes dos ataques chegarem ao sistema operacional do sistema alvo. Pesquisas recentes envolvendo academia e indústria, por exemplo, citam um protótipo de processador para ser usado em *switches* e lidar com fluxos correlatos (em vez de independentes) (LERNER et al., 2024). O desenvolvimento e ampla adoção desse tipo de tecnologia não só trará mais rapidez à comutação de pacotes, mas irá possibilitar o surgimento de tecnologias inovadoras para detecção prévia de ameaças.

O final de 2024 foi marcado pelo lançamento do Willow, o chip quântico da Google, cujas pesquisas estão em andamento há cerca de dez anos (NEVEN, 2024). Os testes feitos para avaliá-lo se mostraram promissores em relação à correção de erros quânticos (ACHARYA et al., 2024), trazendo oportunidades para a demonstração de computação útil (além da fronteira da computação clássica) em aplicações do mundo real e sugere que a criptografia pós-quântica e a criptanálise quântica serão disruptivas. Quando a tecnologia quântica estiver madura a esse ponto, a área da cibersegurança, seja na proteção de sistemas ou em criptografia/criptanálise, irá sofrer profundas transformações que precisarão ser investigadas e avaliadas para que os próximos passos sejam dados e novas tendências sejam levantadas. Em geral, as tecnologias citadas estão no início do ciclo de *hype* e exigem anos para amadurecimento a ponto de serem aplicáveis em cenários reais. Além disso, o *hardware* especializado necessário para implantá-las (como processadores para detecção prévia de ameaças e computação quântica) ainda estão em estágios pouco maduros.

7 Considerações Finais

Este relatório definiu uma visão de futuro na área de cibersegurança, tendo como foco o sistema RNP, os seus gestores governamentais e os seus usuários. Percebe-se que o futuro da cibersegurança envolve questões técnicas e também educacionais, em que é preciso fomentar urgentemente a capacitação em cibersegurança. Nota-se também que é preciso se desenvolver um ecossistema colaborativo entre diversas áreas para alcançar inovação e resiliência em contramedidas aos ciberataques. Não é possível alcançar um ecossistema de cibersegurança duradouro sem a persistente colaboração entre o governo, a indústria e os pesquisadores de cibersegurança na academia. Que este documento sirva de incentivo a essa colaboração.

Referências

ACHARYA, Rajeev et al. *Quantum error correction below the surface code threshold*. 2024. DOI: https://doi.org/10.1038/s41586-024-08449-y.

CISA. *Cybersecurity Strategic Plan FY2024-2026*. 2024.

ENISA. *2024 Report on the State of Cybersecurity in the Union*. 2024.

FORTINET. *2024 Cybersecurity Skills Gap*. 2024.

KUCHARAVY, Andrei et al. *Large Language Models in Cybersecurity: Threats, Exposure and Mitigation*. Springer Cham, 2024.

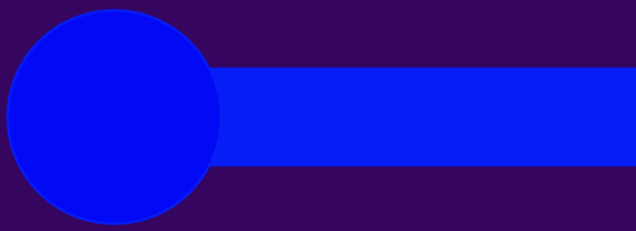
LERNER, Alberto et al. Rethinking the Switch Architecture for Stateful In-network Computing. In: PROCEEDINGS of the 23rd ACM Workshop on Hot Topics in Networks. Irvine, CA, USA: Association for Computing Machinery, 2024. (HotNets '24), p. 273–281. ISBN 9798400712722. DOI: 10.1145/3696348.3696897. Disponível em: <https://doi.org/10.1145/3696348.3696897>.

NEVEN, Hartmut. *Meet Willow, our state-of-the-art quantum chip*. Dez. 2024. https://blog.google/technology/research/google-willow-quantum-chip/.

TRIBUNAL DE CONTAS DA UNIÃO. *Lista de Alto Risco da Administração Pública Federal*. 2024. https://sites.tcu.gov.br/listadealtorisco/index.html.

U.S. BUREAU OF LABOR STATISTICS. *Occupational Outlook Handbook - Information Security Analysts*. 2025. Disponível em: <%5Curl%7Bhttps://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm%7D>.

ZIMMERMANN, Jamie et al. Approaches to improve preprocessing for Latent Dirichlet Allocation topic modeling. *Decision Support Systems*, v. 185, p. 114310, 2024. ISSN 0167-9236. DOI: https://doi.org/10.1016/j.dss.2024.114310. Disponível em: <https://www.sciencedirect.com/science/article/pii/S016792362400143X>.



RNP

MINISTÉRIO DA **CULTURA**

MINISTÉRIO DA **DEFESA**

MINISTÉRIO DA **SAÚDE**

MINISTÉRIO DAS **COMUNICAÇÕES**

MINISTÉRIO DA **EDUCAÇÃO**

MINISTÉRIO DA **CIÊNCIA, TECNOLOGIA E INOVAÇÃO**

GOVERNO FEDERAL
BRASIL
UNIÃO E RECONSTRUÇÃO