Inter-American Defense College

November 6th and 7th 2019

Índice

Colegio Interamericano de Defensa

Inter-American Defense College

Director:
Major General
James E. Taylor, U.S. Army

Vice Director:
Rear Admiral
Sílvio Luís dos Santos, Brazilian Navy

Jefe académico / Chief of Studies:
Brigadier General D.E.M.
Rubén Darío Díaz Esparza, Mexican Army

Editors / Editores
Colombo, Adamo, Col, (BR), IADC
adamo.colombo@iadc.edu

Gil, Jhon, Col, (COL), IADC
jhon.gil@iadc.edu

Asistente de Edición / Editing assistant:
Dra. Sarivette Ortiz, IADC
sarivette.ortiz@iadc.edu

Diseño / Design:
Gil, Jhon, Col, (COL), IADC
jhon.gil@iadc.edu

ISBN – 978-1-7344081-0-2 (Print)
ISBN – 978-1-7344081-1-9 (Online)

Nota Editorial

Atualmente, o tema de Defesa Cibernética é considerado, globalmente, em alta prioridade para a segurança dos Estados, em função do amplo espectro que engloba os efeitos de possíveis ataques cibernéticos em toda a infraestrutura de um país. Por isso, as Forças de Segurança, sejam de Defesa ou de Segurança Pública, têm buscado criar estruturas de resposta, como centros de ensino e comandos de Defesa Cibernética para fazer frente à essa nova e preocupante ameaça.

Alinhado com essa situação, a Organização dos Estados Americanos (OEA), por intermédio do Comitê Interamericano de Combate ao Terrorismo (CICTE), que é o reponsável pela temática de Defesa Cibernética, desenvolve projetos e capacita recursos humanos nessa área específica, demostrando a relevância do assunto em pauta. Recentemente, a Junta Interamericana de Defesa (JID), entidade vinculada à OEA, recebeu a atribuição, por meio do Mandato da Assembleia Geral 2945 (XLIX-O / 19), de realizar um Seminário de Defesa Cibernética, visando ampliar os conhecimentos do pessoal militar no tocante a esse assunto.

Dessa forma, a realização do Seminário de Defesa e Segurança Cibernética, nos dias 6 e 7 de novembro de 2019, pelo Colégio Interamericano de Defesa (CID), em coordenação com a JID, permitiu o cumprimento do referido mandato, bem como, mais importante, possibilitou a difusão e a discussão alusiva ao tema, fortalecendo os mecanismos de cooperação e promovendo o desenvolvimento de políticas e estratégias de Defesa Cibernética.

General de Divisão (Exército Brasileiro)
LUCIANO JOSÉ PENNA
Presidente do Conselho de Delegados da
Junta Interamericana de Defensa

Foreword

On November 6 and 7 of 2019, the Inter-American Defense College (IADC), in concert with the Inter-American Defense Board (IADB), conducted a Cyber Defense and Security Seminar in Washington, DC, which was a direct continuation of the Cyber Conference held by the IADB on May 14 and 16 of 2019 in Colombia.

The mission of the college to prepare the future strategic leaders of the hemisphere is important and beneficial to our collective security and defense. The challenges and threats that face the countries of this hemisphere are complex. They transcend national boundaries. They encompass multiple domains. One nation, alone, cannot solve them. International problems require international solutions. Hemispheric problems require hemispheric solutions. The IADC fostered collaboration by addressing the Cyber aspect of these problems through this event.

This seminar shared best practices and lessons learned, within the scope of the IADB, to promote the development of Cyber Defense policies and strategies, as well as strengthen cooperation mechanisms in Cyber Defense across the Hemisphere.

Furthermore, this seminar directly supported Organization of American States (OAS) AG/RES. 2945 (XLIX-O/19) which addresses cross-cutting themes in support of the four pillars of Democracy, Human Rights, Security, and Development. Participating countries shared best practices of Cyber Security and Cyber Defense in furtherance of the objectives of this resolution.

The analysis of the following presentations allowed us to identify several points of common effort and overarching conclusions, which are addressed in the final article, written by the IADC Cyber Professor Colonel Joao Carneiro, PhD.

These proceedings are intended to enhance hemispheric knowledge of Cyber Security and Defense operations that was discussed during the seminar. They serve as a reference source for academic research. The IADB will promote a new round of conferences on the theme in 2020. With this publication we hope to contribute to defining the issues to be addressed, allowing for enriched understanding of this critical domain.

The Cyber domain is critical to the functioning of society. Nations must secure and defend it. The IADC is proud to present this publication to broaden the hemisphere's understanding of this complex problem and, perhaps, enable agile and creative solutions.

Major General (US Army)
JAMES E. TAYLOR
26th Director of the Inter-American Defense College

El **Capitán de Navío Omar Bracamontes Cruz** Es oficial de superficie, con el Título de Ingeniero en Ciencias Navales. Se ha desempeñado en diversas Unidades de superficie de la Armada de México, fue Jefe del grupo de transferencia del buque R/V "KNORR" a la Armada de México, en Woods Hole, Massachusetts y posteriormente, Comandante de ese buque. Realizó la Maestría en Administración Naval; asimismo, realizó Maestría en Defensa y Seguridad Hemisférica en este Colegio, integrante de la Clase 58. Actualmente, está comisionado en la JID como asesor de la Presidencia del Consejo de Delegados.

LA JUNTA INTERAMERICANA DE DEFENSA, SUS MANDATOS Y OBJETIVOS EN CIBERDEFENSA

Notas de la presentación suministradas por el Capitán de Navío Bracamontes

De acuerdo con el Estatuto de la Junta Interamericana de Defensa (JID), aprobado por la Asamblea General de la Organización de Estados Americanos (OEA) en 2006, la JID es una de las Entidades de la Organización.

Su propósito es prestar a la OEA y a sus Estados Miembros, servicios de asesoramiento técnico, consultivo y educativo sobre temas relacionados con asuntos militares y de defensa en el Hemisferio para contribuir al cumplimiento de la Carta de la OEA.

Para este propósito, la JID deberá tener en cuenta las necesidades de los Estados más pequeños, cuyo grado de vulnerabilidad es mayor frente a las amenazas tradicionales y las nuevas amenazas, preocupaciones y otros desafíos.

La estructura de la JID consiste de tres órganos: el Consejo de Delegados, la Secretaría y el Colegio Interamericano de Defensa.

1) El Consejo de Delegados es el órgano representativo superior de la JID y se encarga de elaborar y adoptar las políticas, actividades y directrices de la JID, conforme a las directrices establecidas por la Asamblea General de la OEA, la Reunión de Consulta de la OEA, y el Consejo Permanente de la OEA. El Consejo de Delegados está constituido por: las Delegaciones, el Presidente y el Vice Presidente.

2) La Secretaría es el órgano de asesoramiento y administrativo de la JID. Está constituida por: la Dirección General, la Subsecretaría de Servicios de Asesoramiento y la Subsecretaría de Servicios Administrativos y de Conferencias.

3) Por su parte, la función del Colegio Interamericano de Defensa consiste en desarrollar y proporcionar oportunidades para oficiales militares y funcionarios civiles de los Estados Miembros

de la OEA en la realización de cursos académicos avanzados en temas relacionados con asuntos militares y de defensa, el sistema interamericano, y disciplinas conexas; gozando de autonomía académica para cumplir esta función. El Colegio Interamericano está integrado por un Director, un Sub-Director y un Jefe de Estudios.

Cualquier Estado miembro de la OEA puede adquirir la calidad de Estado miembro de la JID, debiendo tener por lo menos un representante civil o militar acreditado oficialmente como delegado ante el Consejo de Delegados de la JID. Actualmente, de los 34 miembros de la OEA (sin considerar a Cuba[1]), 28 son también miembros de la JID sin embargo, de éstos, Venezuela y Surinam no tienen Delegados acreditados.

En al JID también están como observadores ocho Estados: España, Holanda, Francia, Dinamarca, Italia, Portugal, China y Reino Unido.

La JID goza de autonomía técnica para el cumplimiento de su propósito y funciones, y tiene en cuenta los mandatos de la Asamblea General de la OEA, la Reunión de Consulta de Ministros de Relaciones Exteriores y el Consejo Permanente de la OEA.

Asimismo, coordina constantemente con la Comisión de Seguridad Hemisférica del Consejo Permanente, con la Secretaría de Seguridad Multidimensional, así como con la Comisión Interamericana para Control del Abuso de Drogas (CICAD), el Comité Interamericano Contra el Terrorismo (CICTE) y el Comité Interamericano para la Reducción de los Desastres Naturales (CIRDN).

Derivado de su propósito, la Junta ha establecido un instrumento de gestión con una vigencia de cinco años, denominado Plan Estratégico 2017 – 2021. Este Plan define cinco objetivos estratégicos:

1) Contribuir a la defensa y la seguridad en el hemisferio.

2) Fortalecer la cooperación hemisférica en defensa y seguridad.

3) Expandir el conocimiento sobre seguridad y defensa hemisférica a través de la educación de postgrado, la capacitación y conferencias.

4) Promover la vinculación extra hemisférica en asuntos militares y de defensa.

5) Optimizar el funcionamiento administrativo de la JID.

[1] El 3 de junio de 2009, los Ministros de Relaciones Exteriores de las Américas adoptaron la resolución AG/RES. 2438 (XXXIX-O/09), la cual resuelve que la Resolución de 1962, mediante la cual se excluyó al Gobierno de Cuba de su participación en el sistema interamericano, queda sin efecto en la Organización de los Estados Americanos (OEA). La resolución de 2009 declara que la participación de la República de Cuba en la OEA será el resultado de un proceso de diálogo iniciado a solicitud del Gobierno de la República de Cuba y de conformidad con las prácticas, los propósitos y principios de la OEA.

Del objetivo estratégico número 1 se deriva un objetivo específico que es: Impulsar el desarrollo y elaboración de políticas y/o estrategias de ciberdefensa en el Hemisferio.

Asimismo, dentro de los mandatos de la Asamblea General del cuadragésimo octavo periodo ordinario de sesiones en 2018, en la resolución para la promoción de la seguridad hemisférica se solicitó a la JID realizar un seminario o conferencia sobre ciberseguridad con la finalidad de proponer recomendaciones a los Estados Miembros sobre la seguridad en el manejo de información a través del ciberespacio y la protección de los medios informáticos.

También, en el cuadragésimo noveno periodo ordinario de sesiones de la Asamblea General de la OEA en junio de este año, se solicitó a la JID continuar fortaleciendo los mecanismos de cooperación en defensa cibernética en el Hemisferio realizando, entre otros, una conferencia sobre defensa cibernética, en coordinación con otros órganos, organismos y entidades pertinentes de la OEA.

Derivado de estos Mandatos y Objetivos, es que ampliará sus proyectos e iniciativas de ciberdefensa para complementar los esfuerzos de la OEA en el tema.

General de Divisão Guido Amin. Formado pela Academia Militar das Agulhas Negras (Artilharia), possui mestrado em Operações Militares pela Escola de Aperfeiçoamento de Oficiais e Doutorado em Ciências Militares pela Escola de Comando e Estado-Maior do Exército. Possui o curso de Estado-Maior Conjunto das Forças Armadas da Espanha. Especialista em Relações Internacionais. Comandou o 14º Grupo de Artilharia de Campanha e a 1ª Brigada de Artilharia Antiaérea. Chefiou o Escritório de Projetos do Exército. Foi conselheiro militar da Missão Permanente das Nações Unidas do Brasil em Nova York, Estados Unidos e Observador militar na Missão das Nações Unidas em Moçambique. Atualmente, é comandante do Comando de Defesa Cibernética, Brasília, Brasil.

Coronel Edson Ribeiro dos Santos Jr. PhD. Formado pela Academia Militar das Agulhas Negras (Artilharia), possui mestrado em Operações Militares pela Escola de Aperfeiçoamento de Oficiais e Doutorado em Ciências Militares pela Escola de Comando e Estado-Maior do Exército. É pós-doutorando em Ciências Militares pelo Instituto Meira Mattos. Especialista em Relações Internacionais e possui MBA em gerenciamento de Projetos. Cursou o Captain´s Career Course em Fort Bliss-EUA. Comandou a Escola de Artilharia de Costa e Antiaérea. Atualmente, é assessor de governança e projetos do Comando de Defesa Cibernética, Brasília, Brasil

SEGURANÇA E DEFESA CIBERNÉTICAS: MELHORES PRÁTICAS E LIÇÕES APRENDIDAS

1. Introdução

A Segurança e a Defesa Cibernéticas são assuntos prioritários na agenda dos Estados nos dias atuais. As especificidades do Setor Cibernético caracterizam-se, dentre outros aspectos, pelo ineditismo, pela velocidade de mudanças e pela transversalidade do tema. Esses fatos indicam a necessidade de práticas que possibilitem a efetividade e oportunidade das ações, gerando conhecimentos relevantes para a consolidação e amadurecimento na condução da Defesa Cibernética.

No Brasil, marcos legais do mais alto nível da defesa e da segurança do país têm buscado contemplar a normatização e a segurança jurídica para estruturar e permitir a atuação dos entes do Estado envolvidos no planejamento e ações no Setor.

A Estratégia Nacional de Defesa, já na sua primeira edição de 2008, definiu os três setores estratégicos para a Defesa do Estado Brasileiro: o nuclear, o espacial e o cibernético. A Portaria nº 14 de 2009, do Ministério da Defesa, atribuiu a cada uma das Forças as responsabilidades pelos três Setores Estratégicos. À Marinha do Brasil, coube o Setor Nuclear, à Força Aérea Brasileira, o Espacial e ao Exército, o Setor Cibernético.

Este texto buscará registrar as melhores práticas e lições aprendidas, até o presente momento, na implantação e condução do Setor Cibernético de Defesa do Brasil, sob a responsabilidade do Exército Brasileiro.

2. Desenvolvimento

2.1 Breve Histórico

Podem-se destacar alguns fatos que, cronologicamente, marcaram a evolução da Defesa Cibernética a cargo do Exército Brasileiro até os dias atuais.

Após a definição dos três Setores Estratégicos pela Estratégia Nacional de Defesa, em 2008, e a atribuição da responsabilidade de cada um deles pela Diretriz nº 14 do Ministério da Defesa, em 2009, o Exército criou, no início de 2010, o Projeto Estratégico do Exército Defesa Cibernética (PEE D Ciber) que, com sete subprojetos, tinha por finalidade entregar a estrutura necessária para a execução da missão atribuída pela sociedade.

Uma das primeiras entregas do PEE D Ciber, ainda em 2010, foi o núcleo do Centro de Defesa Cibernética (CDCiber), sediado provisoriamente nas instalações do Quartel General do Exército.

Em 2013, o caso Snowden resultou na implantação de uma Comissão Parlamentar de Inquérito (CPI) no Senado Federal para investigar as denúncias de espionagem externa no governo brasileiro. O relatório da CPI determinou várias medidas a serem implantadas por diferentes setores do governo federal. Uma delas foi a criação de um grupo de trabalho interministerial, sob a coordenação do Ministério da Defesa, para apontar ações concretas que resultassem no fortalecimento da segurança e da Defesa Cibernética.

Neste contexto, o Ministério da Defesa criou, em 2014, o Programa de Defesa Cibernética na Defesa Nacional (PDCDN), constituído por 10 projetos, a ser gerenciado também pelo Exército Brasileiro, mas com recursos diretos do Ministério. No que se refere às iniciativas estratégicas para implantação do Setor Cibernético, portanto, a partir de 2014, passaram a existir o PDCDN e o PEE D Ciber. O primeiro, com verbas do Ministério da Defesa, visa o Setor de Defesa Cibernética como um todo, já o segundo, com recursos orçamentários do Exército, tem por objetivo atender às demandas cibernéticas da Força Terrestre.

Os resultados do PDCDN começaram a aparecer já em 2015, quando foram criados os núcleos do Comando de Defesa Cibernética e da Escola Nacional de Defesa Cibernética, localizados, inicialmente, nas instalações do Quartel General do Exército. Ambas as entregas

constavam das determinações da CPI do Senado Federal e do Grupo de Trabalho Interministerial coordenado pelo Ministério da Defesa.

Em 2016, após a assunção de seu primeiro comandante, o Comando de Defesa Cibernética (ComDCiber) deixou de ser núcleo e passou a enquadrar o Centro de Defesa Cibernética e o Núcleo da Escola Nacional de Defesa Cibernética. Em 2017, o ComDCiber saiu das instalações do Quartel General do Exército e ocupou suas atuais instalações no Forte Marechal Rondon. O que também aconteceu com a Escola Nacional de Defesa Cibernética em fevereiro de 2019, que deixou de ser núcleo e passou a ser uma Organização Militar diretamente subordinada ao ComDCiber, também no Forte Marechal Rondon.

Cumpre destacar que toda esta estruturação foi impactada com a atuação em operações reais nos grandes eventos ocorridos desde 2010 até 2016, quais sejam: a Conferência das Nações Unidas sobre Desenvolvimento Sustentável, conhecida por Rio +20; a Jornada Mundial da Juventude, com a presença do Papa Francisco; a Copa das Confederações; a Copa do Mundo; e, finalmente os Jogos Olímpicos de 2016. Em todos os eventos citados, houve a participação do Setor Cibernético de Defesa, coordenando as operações conjuntas e interagências. Apenas para que se tenha noção, somente durante a Copa do Mundo, houve 756 eventos de segurança cibernética que requereram algum tratamento.

Desta evolução, alguns ensinamentos foram importantes. Destacam-se: a imprescindibilidade de se trabalhar com uma metodologia de gerenciamento de programas e projetos para que entregas complexas sejam obtidas, com tempestividade, em um planejamento alinhado com os objetivos estratégicos; e a capacidade de trabalhar em um ambiente colaborativo interagências, obtendo sinergia com os pontos fortes de cada um dos atores e mitigando os pontos fracos dos partícipes. Só assim é possível fortalecer o ecossistema como um todo, diminuindo as vulnerabilidades e obtendo a velocidade de respostas requerida.

2.2 Marcos Legais e Normatização

Após a Estratégia Nacional de Defesa, o Setor Cibernético passou a ser normatizado. Dentre os documentos mais relevantes, destacam-se:

- A Política Cibernética de Defesa, de 2012, que tem a finalidade de orientar, no âmbito do Ministério da Defesa (MD), as atividades de Defesa Cibernética, no nível estratégico, e de Guerra

Cibernética, nos níveis operacional e tático, visando à consecução dos seus objetivos. A Política Cibernética de Defesa aplica-se a todos os componentes da expressão militar do Poder Nacional, bem como às entidades que venham a participar de atividades de Defesa ou de Guerra Cibernética.

- A Doutrina Militar de Defesa Cibernética, de 2014, tem por finalidade estabelecer os fundamentos doutrinários do Setor, proporcionando unidade de pensamento sobre o assunto, no âmbito do Ministério da Defesa (MD), e contribuindo para a atuação conjunta das Forças Armadas (FA) na defesa do Brasil no espaço cibernético.

Tanto a Política Cibernética de Defesa, quanto a Doutrina Militar de Defesa Cibernética foram documentos elaborados pelo Ministério da Defesa.

- Em 2015, o Gabinete de Segurança Institucional (GSI) da Presidência da República, publicou a Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal. Este documento tem por finalidade apresentar as diretrizes estratégicas para o planejamento de segurança da informação e comunicações e de segurança cibernética no âmbito da Administração Pública Federal (APF), objetivando a articulação e a coordenação de esforços dos diversos atores envolvidos, de forma a atingir o aprimoramento da área no Governo e a mitigação dos riscos aos quais se encontram expostas as organizações e a sociedade.
- A Política Nacional de Defesa (PND), na edição de 2016, fixa os objetivos da Defesa Nacional e orienta o Estado sobre o que fazer para alcançá-los. É o documento condicionante de mais alto nível do planejamento de ações destinadas à defesa nacional coordenadas pelo Ministério da Defesa. Voltada essencialmente para ameaças externas, estabelece objetivos e orientações para o preparo e o emprego dos setores militar e civil em todas as esferas do Poder Nacional, em prol da Defesa Nacional. Ratificando versões anteriores, a PND define que “para que o desenvolvimento e a autonomia nacionais sejam alcançados é essencial o domínio crescentemente autônomo de tecnologias sensíveis, principalmente nos estratégicos setores espacial, cibernético e nuclear.”
- Ainda em 2016, foi publicada uma nova versão do Livro Branco de Defesa Nacional. Este documento ratifica os Setores Estratégicos da Defesa Nacional e define as Iniciativas Estratégicas, sob gerenciamento do Exército Brasileiro, para estruturar e obter os meios necessários do Setor Cibernético de Defesa.
- A Política Nacional de Segurança da Informação (PNSI), publicada em 2018, dispõe sobre a governança da informação no âmbito da administração pública no âmbito da Administração

Pública Federal. A PNSI tem por finalidade assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional. Este documento determina ao Ministério da Defesa que elabore as diretrizes, os dispositivos e os procedimentos de defesa que atuem nos sistemas relacionados à defesa nacional contra ataques cibernéticos.

- O Gabinete de Segurança Institucional da Presidência da República (GSI/PR), órgão do governo brasileiro responsável pelo assessoramento do presidente sobre assuntos militares e/ou de segurança, considerou a área de proteção cibernética como sendo a mais crítica e atual a ser tratada. Em janeiro de 2019, foi eleita a Estratégia Nacional de Segurança Cibernética (ou E-Ciber) como o módulo inicial da estratégia nacional para a salvaguarda da informação, após ter contado com a participação de diversas entidades públicas e privadas do país. A Estratégia Nacional de Segurança Cibernética está em fase final de elaboração. Esse planejamento, levando em consideração a amplitude da área de proteção dos dados, será produzido em módulos, a fim de se contemplar os seguintes pontos:

    - Segurança Cibernética
    - Defesa Cibernética
    - Segurança das Infraestruturas Críticas
    - Segurança da Informação Sigilosa
    - Proteção Contra Vazamento de Dados

- A Estratégia Nacional de Segurança Cibernética estabelecerá “o quê” fazer. No prosseguimento à consolidação da normatização do Setor Cibernético, serão definidas as atribuições e os responsáveis por cada uma das ações necessárias. É neste contexto que se prevê o Plano Nacional de Defesa Cibernética que, juntamente com outros planos congêneres, definirá, no que se refere ao Setor de Defesa, “como, quando e quem” serão os executores de cada uma das ações necessárias.

No âmbito do Ministério da Defesa, além da Política Cibernética de Defesa e da Doutrina Militar de Defesa Cibernética, encontra-se em revisão a Doutrina de Operações Conjuntas, com participação efetiva de militares do ComDCiber, particularmente na atualização do Capítulo VIII – Comando de Defesa Cibernética e do Capítulo XII – Defesa Cibernética nas Operações Conjuntas. Para esse trabalho e visando à normatização do Setor Militar de Defesa Cibernética, merece destaque o Workshop Doutrinário do Sistema Militar de Defesa Cibernética, realizado pelo ComDCiber em outubro de 2019. Nessa atividade, representantes das três Forças, do Ministério

da Defesa, do GSI e de outras agências puderam expor suas ideias e contribuir para a atualização normativa em curso.

Da análise dos marcos legais, infere-se a importância de normas que amparem os agentes do Estado nas ações necessárias a sua defesa. Ademais, e tão importante quanto, é fundamental otimizar competências de órgãos distintos da estrutura governamental e da iniciativa privada, em especial das infraestruturas críticas. Mais uma vez, observa-se que a velocidade que caracteriza o Setor Cibernético revela-se em grande desafio para que normas dependentes de processos complexos sejam tempestivas e eficazes.

2.3 Estrutura do Setor Cibernético Brasileiro

Em que pese a elaboração de novos marcos legais, já está estabelecida a estrutura do Setor Cibernético Brasileiro, com os atores mais relevantes e os respectivos níveis de decisão. A Doutrina Militar de Defesa Cibernética consolida esta estrutura.

No nível político, o principal ator é o Gabinete de Segurança Institucional da Presidência da República (GSI-PR). Dentre outras atribuições, no que se refere ao Setor Cibernético, cabe ao GSI a segurança da informação e a segurança cibernética da Administração Pública Federal, além da segurança cibernética das infraestruturas críticas. Neste nível, preponderam as atividades de ‘proteção’ cibernética. Ainda na esfera política, merece registro a Secretaria de Assuntos Estratégicos da Presidência da República (SAE), como formulador de políticas de segurança do mais alto nível do Estado, tem se preocupado em apoiar a inserção da Segurança Cibernética como um dos assuntos estratégicos mais relevantes para o país.

No nível estratégico, o Ministério da Defesa e os Comandos das Forças assumem o protagonismo das ações. É neste nível que o Comando de Defesa Cibernética atua, como órgão central do Sistema Militar de Defesa Cibernética. O principal interlocutor do ComDCiber no Ministério da Defesa é o Estado-Maior Conjunto das Forças Armadas. A partir do nível estratégico, observa-se a mudança do viés exclusivo de segurança cibernética para a defesa cibernética. Embora medidas de segurança sejam implementadas em todos os níveis, a defesa implica que, além da proteção, a exploração e o ataque são executados neste nível, em cumprimento às demandas das autoridades competentes.

No nível operacional, uma vez estabelecido um comando operacional conjunto, o ComDCiber atuará em ações específicas e organizará a Força Cibernética Componente, seja enviando seus militares próprios, ou solicitando a mobilização de agentes de estruturas diversas, o que é decorrente de um controle de especialistas gerenciado pelo ComDCiber. Neste nível, ocorrem as ações de guerra cibernética.O nível tático é caracterizado pela ação das Forças Componentes. Consequência do planejamento operacional, uma Força Conjunta de Guerra Cibernética atua nas ações ad hoc de guerra cibernética.

Observa-se que, em todos os níveis citados, a única organização que trata exclusivamente de Defesa Cibernética de forma permanente é o Comando de Defesa Cibernética, fato que demanda sua atuação em todo o espectro, do político ao tático.

A estrutura apresentada mostra-se adequada à realidade e serve de base para que o detalhamento necessário para a normatização alcance a maturidade requerida.

2.4 Melhores Práticas e Lições Aprendidas

Uma vez compreendida a estrutura e os principais marcos legais que norteiam o Setor Cibernético de Defesa no Brasil, considerando também os ensinamentos obtidos nas operações desencadeadas nos grandes eventos, é possível discorrer sobre atividades recentes que resultaram em práticas geradoras de resultados importantes.

Em paralelo às atividades cotidianas do ComDCiber, a partir do final de 2017 até meados de 2018, foi realizado um trabalho de análise do Setor Cibernético de Defesa. Esta análise teve início com um diagnóstico, cujos principais aspectos observados e resultados obtidos foram:

- governança: verificou-se a necessidade de melhorar a governança do Setor. A transversalidade inerente ao Setor resulta num grande número de atores com múltiplas linhas de comando e subordinação e com enfoques nem sempre convergentes em relação a prioridades, produtos a serem obtidos, ações a serem implementadas e tantos outros aspectos. Ainda que se entenda a legitimidade de cada um dos posicionamentos, há um momento em que, para que se obtenham os resultados necessários, haja a definição de uma cadeia decisória com atribuições claras a cada nível;
- relações institucionais: a multiplicidade de atores envolvidos leva ao entendimento da relevância do aspecto colaborativo no Setor Cibernético não pode ficar circunscrito à retórica. A Defesa do Estado, particularmente no que se refere à cibernética, depende cada vez mais de estabelecimento de relacionamentos de toda ordem, com atores nacionais e internacionais, dentro e fora do setor de defesa. Insere-se aí a importância de atores do nível estratégico. Muitas vezes, o apelo técnico inerente à tecnologia da informação limita o estabelecimento de parcerias a este nível, que é importante, mas não pode ser exclusivo;
- gestão: o Exército já havia optado por uma metodologia própria de gerenciamento de iniciativas estratégicas. A análise, porém, foi importante para avaliar a pertinência dos produtos planejados com a realidade operacional que se impõe. Ainda no que se refere à gestão, os reflexos das questões relacionadas à governança se mostraram importantes na definição dos rumos das iniciativas estratégicas. Neste contexto, considerando-se ainda a multiplicidade de atores e a presteza requerida no Setor Cibernético, há de se buscar uma inovação na gestão, englobando a governança, relações público-privadas e processos de contratação pública;
- estruturas e processos: a experiência obtida nos grandes eventos e o amadurecimento resultante das atividades diárias levaram a uma reflexão em relação a processos e estrutura. Observaram-se oportunidades de melhoria resultantes de um mapeamento detalhado do que se fazia e o confronto com o que se necessita fazer no futuro próximo. Processos foram melhorados e criados, permitindo o levantamento detalhado de pessoas e sistemas necessários para o cumprimento da missão do ComDCiber. Para que se atingissem esses resultados, foi contratada uma empresa nacional, que,

de forma científica, construiu, com os integrantes do ComDCiber, a cadeia de valor e a arquitetura de processos;

- doutrina e normativa: aspecto já abordado anteriormente, mas que mereceu atenção na análise, permitindo identificar lacunas de amparo às ações e necessidades de formalização de procedimentos já em execução;
- recursos: como já demonstrado, num primeiro momento, o Exército alocou recursos orçamentários próprios para atender às demandas iniciais da estruturação do Setor. Mais adiante, o próprio Ministério da Defesa passou a alocar recursos diretamente para um dos Programas. Observou-se, porém, a necessidade de estruturação da demanda focada na vertente operacional para que se obtivessem valores coerentes com a prioridade estratégica atribuída pelo próprio Estado Brasileiro e compatíveis com os valores destinados aos demais setores estratégicos.

Ao término do diagnóstico resumidamente apresentado acima, algumas consequências foram enumeradas, das quais três mostraram-se mais relevantes:

- risco real: os acontecimentos mostravam eventos de natureza e gravidade distintas ocorrendo diuturnamente, ao tempo em que foram observadas lacunas de capacidades para combater de forma efetiva as ameaças. As ações empreendidas mostravam-se adequadas, mas a certeza da evolução e da velocidade de mudança da ameaça indicavam a necessidade de implementar mudanças e fechar vulnerabilidades tão rápido quanto possível;
- setor desequilibrado: constatou-se que o Setor Cibernético é o mais transversal a todas as atividades do Estado e sem a prioridade adequada em relação aos demais setores. Paradoxalmente, verificou-se um desequilíbrio entre capacidades disponíveis e recursos aplicados. Há abundância de soluções técnicas e uma quantidade de pessoal capacitado para lidar com ameaças que, se não o ideal, em número que permite operar com segurança. Nos níveis operacional e, particularmente, estratégico, há o que se fazer tendo em vista a necessidade de marcos legais adequados. O mesmo ocorria no nível político, onde o Setor Cibernético carecia de uma inserção adequada;
- percepções distintas: durante os trabalhos, percebeu-se uma diversidade de posicionamentos, não apenas com enfoques diferentes, mas também com distanciamento da realidade. Em determinadas áreas, priorizaram-se aspectos abstratos em detrimento de obtenção de produtos eminentemente operacionais requeridos pela realidade dos acontecimentos. Há de se identificar a quem e como caberá o fomento de pesquisas e discussões em torno da evolução de tecnologias e, em outra vertente, a execução de projetos que busquem entregas necessárias ao enfrentamento de

ameaças concretas do campo operacional. Ambos os vieses são importantes, mas, voltando à governança, alguém tem que emitir prioridades, definir responsabilidades e chegar a resultados concretos. Na mesma lógica, verificou-se percepções distintas de atores externos, com omissões na tomada de iniciativas, muitas vezes por parte de quem deve ser protegido, ou intromissão de forma não adequada por operadores de tecnologia da informação, que, muitas vezes, não possuem uma visão holística do cenário cibernético.

Como resultado, verificou-se que as decisões tomadas desde 2009 quando da criação do Setor Cibernético de Defesa foram acertadas e coerentes com as circunstâncias e a maturidade disponível em cada momento. As capacidades obtidas durante a implantação do Setor permitiram o atingimento da percepção que essa busca por capacidades cibernéticas é um processo sem fim. Identificou-se, porém, que a consolidação do Setor depende da inserção do tema na agenda política e estratégica do país. Esta é uma das prioridades atuais estabelecidas pelo ComDCiber.

Do diagnóstico realizado e da prioridade citada, decorreram diversas ações, cujos resultados e melhores práticas já podem ser enumerados:

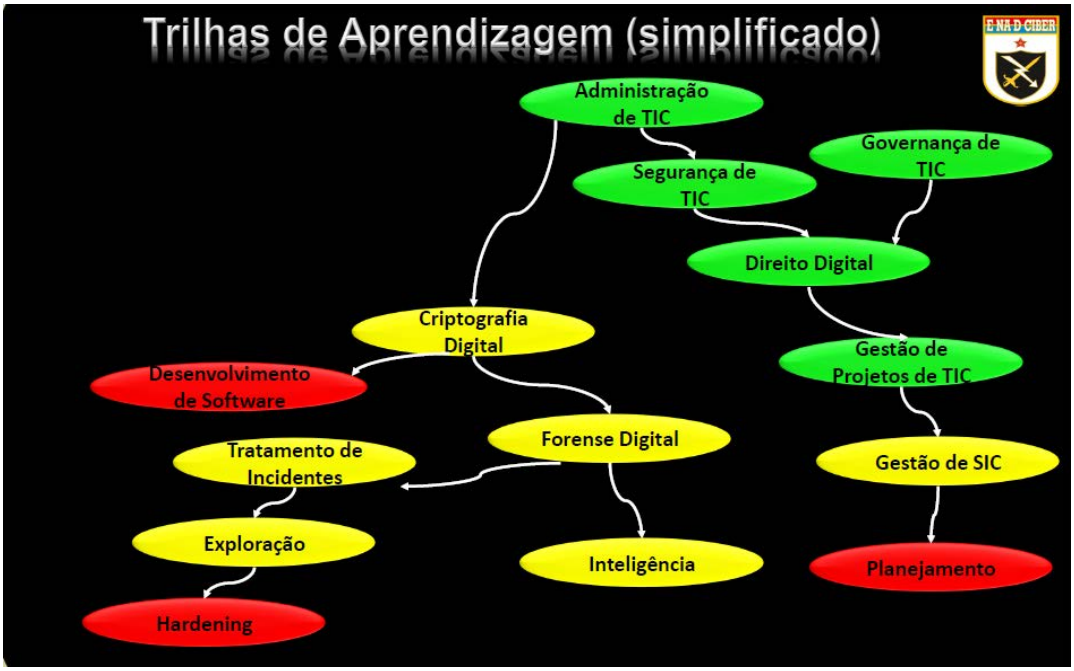
- governança: embora não seja tão simples quanto parece, considerando-se as especificidades do meio militar, a diversidade de atores impactados pelo Setor Cibernético gera uma multiplicidade de interesses que, embora legítimos, nem sempre são convergentes. O apoio da alta administração das Forças e de decisores externos para a definição da autoridade compatível com a responsabilidade atribuída é fundamental para a obtenção de resultados necessários. No caso específico, uma vez identificado o problema, houve a necessidade de designar um ‘gerente executivo de implantação do Setor’, com a autoridade para promover as ações que se impõem. Outro exemplo digno de registro foi a estruturação do Sistema Militar de Defesa Cibernética (SMDC), definindo processos e responsabilidades dos integrantes do SMDC. Para tanto, os Programas Estratégicos, que se constituem nas iniciativas indutoras do processo de transformação, foram reavaliados e reestruturados a fim que pudessem entregar os produtos e efeitos necessários para os objetivos estabelecidos;
- participação em exercícios nacionais e internacionais: os exercícios permitem que a estrutura seja desafiada e seus integrantes testados em cenários diversos. A gestão do conhecimento obtido é essencial para a melhoria contínua dos quadros e aprimoramento dos processos e da própria estrutura existente;

- interação com atores diversos: sabe-se que ‘colaboração’ é uma das palavras mais citadas na literatura sobre cibernética. É fundamental que este fato vá além da retórica e se traduza em prática. A integração de atores deve preceder à integração de processo, sejam eles simples ou complexos. A segurança do ecossistema como um será diretamente proporcional ao nível de interação que os integrantes desse ecossistema possuem entre si;
- cooperação e integração com a proteção das Infraestruturas Críticas (IEC): ainda que possa estar inserido no aspecto anterior, o destaque da relação com as IEC deve-se à particularidade que, no caso do Brasil, tratam-se também de entes privados. Portanto, a regulamentação não é fácil. Não apenas pela natureza privada, mas pela diversidade de áreas. Cresce mais ainda de importância o entendimento da necessidade do ambiente colaborativo. Destaca-se, porém, o excelente nível de relacionamento obtido, fundamentado por confiança e respeito mútuo. O ComDCiber orgulha-se de ser um catalizador no estabelecimento desta rede, como será demonstrado mais adiante ao descrever o Exercício Guardião Cibernético;
- trabalho conjunto e interagências: as operações executadas durante os grandes eventos foram o alicerce para o aprendizado de se trabalhar conjuntamente com as Forças coirmãs e, particularmente, com as diferentes agências da administração pública federal e privadas. A exata medida de se aprender a coordenar, sem impor, e chegar a resultados contra ameaças concretas não é ciência. É arte. Num ambiente estritamente militar, as relações hierarquizadas são parte da cultura. Mas quando se envolvem instituições civis em operações de não-guerra há de se saber operar para alcançar os objetivos comuns;
- cabe um registro de uma iniciativa prática que envolve os últimos atores aqui citados. Uma ferramenta de compartilhamento de inteligências de ameaças permitiu uma maior aproximação, consolidação dos contatos estabelecidos e obtenção de resultados práticos;
- o trabalho com a metodologia de gerenciamento de iniciativas estratégicas do Exército mostrou a importância de definir, cientificamente, o que se necessita. O levantamento de requisitos, ao mesmo tempo em que conduz à sistematização do conhecimento gerado, contribui decisivamente para o amadurecimento dos integrantes do sistema. Em paralelo, permite uma segurança jurídica, administrativa e de efetividade para a celebração de contratações complexas e custosas. Observe-se, porém, que os requisitos devem ser de efeito, traduzindo resultados esperados, ao invés de soluções pontuais que atendam às ameaças do presente, mas poderão não funcionar com cenários do futuro;

- busca do consenso: embora possa parecer paradoxal em relação às ideias apresentadas no aspecto ‘governança’, observa-se que as soluções resultantes do consenso são mais perenes e mais fáceis de serem implementadas do que aquelas que, por falta do consenso, tiveram que ser impostas. Isto é fato tanto para o ambiente interno, quanto o externo.
- horizonte de planejamento: muito já se falou da velocidade de mudança que caracteriza o Setor Cibernético. Os planejamentos, essenciais para que se obtenham resultados concretos, são impactados pela mutabilidade do cenário e das ameaças. Nos níveis operacional e estratégico, a prática tem mostrado que este horizonte é de cinco anos.

Além dos aspectos já citados, merece destaque o preparo cognitivo do pessoal que lidará com o Setor Cibernético nas diferentes vertentes. Neste contexto, a Escola Nacional de Defesa Cibernética criou um sistema educacional que resultou nas ‘trilhas de aprendizagem’. Trata-se de num trabalho multidisciplinar que envolveu pedagogos, especialistas em tecnologia da informação, em defesa cibernética e em outras áreas. As trilhas de aprendizagem são módulos de disciplinas, as quais se constituem no menor caminho para desenvolver as competências necessárias para o Setor Cibernético.

As trilhas definem os domínios temáticos, os perfis profissiográficos e as competências a serem trabalhadas.



A figura acima apresenta uma visão simplificada de algumas capacitações. As cores indicam os níveis básico (verde), intermediário (amarelo) e avançado (vermelho). Observa-se que,

com o mapeamento das trilhas, obtém-se a visualização das competências necessárias para que atinja diferentes níveis de capacitação. Isso também permite otimizar o processo educativo, na medida em que um profissional já possuidor de um conhecimento específico pode acessar o curso necessário para avançar na sua especialização sem a necessidade de ir para o início do processo.

Ainda no que se refere à capacitação, merece registro a contratação de cerca de 1200 cursos para militares, no Brasil e no exterior, comprovando, na prática, a importância atribuída pelo ComDCiber ao aperfeiçoamento dos seus quadros.

Em 2020, a Escola Nacional de Defesa Cibernética atenderá não apenas o público militar, mas oferecerá cursos para servidores civis do Estado Brasileiro.

2.5 Atividades mais relevantes com a participação do ComDCiber

A fim de exemplificar o que foi descrito no item anterior, julga-se pertinente citar atividades de maior destaque que trouxeram lições aprendidas e permitiram a execução de melhores práticas.

A busca por participação em atividades com atores internacionais é cada vez maior. Apenas em 2019, dentre outras que poderiam ser citadas, registra-se: a participação no III Exercício Ibero-Americano de Defesa, que ocorrerá em novembro no Brasil; o Estágio Internacional de Defesa Cibernética, realizado no Brasil em maio; o III Fórum Ibero-Americano, sediado no Brasil em abril; a participação no Exercício Locked Shields, com uma equipe de militares do ComDCiber integrando o time espanhol, em abril, na Espanha, e a visita à direção do Exercício na Estônia; a participação na International Conference on Cyber Conflict, também na Estônia, em maio; assim como a presença na Cycon, nos Estados Unidos em novembro.

No que se refere à inserção do Setor Cibernético no nível político-estratégico, merecem destaque ações que visavam à integração com outros órgãos do Ministério da Defesa, com o Governo Federal, com o setor privado e com a comunidade acadêmica. Como exemplos, citam-se a celebração de acordos e parcerias com institutos e universidades; reuniões com o Grupo de Trabalho Interforças, constituído por representantes das Forças coirmãs e pelo Ministério da Defesa; encontro de especialistas, envolvendo setores do governo e da iniciativa privada; e várias participações em audiências no Congresso Nacional.

O ComDCiber participa de todas as Operações Conjuntas do Ministério da Defesa, desde a fase de planejamento até a fase de execução, mobiliando, com seu próprio pessoal as diferentes

células do Estado-Maior operacional, além do comando da Força Conjunta de Guerra Cibernética (F Cj G Ciber).

O mesmo ocorre na participação nas operações reais de Garantia da Lei e da Ordem, enviando equipes especializadas para onde se fizer necessário, ou desencadeando ações desde a sede do próprio Comando.

O ComDCiber toma a iniciativa na condução de planejamento e execução de exercícios interagências, envolvendo diferentes setores da Administração Pública Federal e do setor privado.

O exemplo mais significativo, que congrega uma quantidade significativa de atores, é o Exercício Guardião Cibernético, cuja segunda edição ocorreu de 2 a 4 de julho de 2019, no Comando de Defesa Cibernética (ComDCiber). Este ano, a atividade envolveu a proteção cibernética, por meio da atuação colaborativa das Forças Armadas, de Órgãos Parceiros e das infraestruturas críticas dos setores de Defesa, Elétrico, Financeiro, Nuclear e de Telecomunicações, e adota técnicas de simulações virtual e construtiva.

A simulação virtual utilizou o programa Simulador de Operações Cibernéticas (SIMOC), no qual foram emulados sistemas computacionais utilizados pelos especialistas dos órgãos e empresas participantes. A simulação construtiva empregou gabinetes de crise das áreas de tecnologia da informação, comunicação social, jurídica e alta administração, que apresentaram soluções para os eventos cibernéticos com impacto nas organizações. As discussões nos gabinetes de crise demandaram ações nos níveis decisório-gerencial (gestão de crise) e técnico (resposta ao incidente).

Participaram do exercício representantes dos seguintes órgãos, instituições e empresas: Ministérios da Defesa, da Justiça e das Relações Exteriores; Gabinete de Segurança Institucional da Presidência da República; Marinha, Exército e Força Aérea; órgãos do Governo Federal; Banco Central do Brasil; bancos públicos e privados; empresas do setor nuclear elétrico e de telecomunicações e comunidade acadêmica. No total, foram 215 participantes, das 41 organizações citadas.

Os participantes atuaram de forma colaborativa e integrada nos esforços voltados para prevenir e solucionar incidentes, envolvendo ativos da informação de relevância para a Defesa Nacional. Por meio do exercício, o ComDCiber busca contribuir para a integração entre governo, setor privado e meio acadêmico no incremento da proteção do espaço cibernético nacional.

Buscou-se demonstrar que as atividades mais recentes e relevantes que tiveram a participação do ComDCiber estão inseridas num contexto maior, com objetivos definidos de inserção do tema no nível político-estratégico e o aumento da rede de relacionamentos, com foco na celebração de parcerias que resultem em colaborações efetivas.

3. Conclusão

Constata-se que o ComDCiber, a despeito de ser uma organização militar muito nova, conseguiu avançar na implantação do Setor Cibernético de Defesa Brasileiro. A dinâmica das ações implementadas, permeada pela característica de constante mutação de cenário, permitiu que se obtivessem lições aprendidas e identificassem melhores práticas.

Resumidamente, destacam-se os seguintes aspectos:

- busca do consenso: é sempre o melhor caminho a ser buscado. Decisões impostas tendem a ser menos duradouras e encontram resistências na execução. A abertura para o diálogo deve ser uma constante;
- mais que conjunta, a estrutura deve prever ser interagências. O ambiente colaborativo é fundamental para o sucesso e fortalecimento do ecossistema. Ainda que o viés seja militar, o ambiente cibernético não se coaduna com limites rigidamente definidos, o que implica na imprescindibilidade de abrir espaço para agências civis nas operações militares;
- transversalidade, com múltiplos atores e atividades: a cibernética impacta em todos os setores da sociedade. São entidades governamentais e privadas, com diversidade de interesses e motivações. A compreensão desse cenário, embora nem sempre seja suficiente para solucionar todos os problemas, é fundamental para que se alcancem resultados importantes;
- capacitação e adestramentos constantes: a velocidade de mudança é inerente à natureza da cibernética. Isto implica na necessidade de processos de capacitação e adestramento permanente. A participação em exercícios diversos permite que cenários fictícios sejam utilizados para testar estruturas, planejamentos e processos, chegando a lições aprendidas relevantes, que contribuem para a capacitação dos integrantes das organizações;
- otimização da capacitação: as trilhas de conhecimento mostraram ser um instrumento eficaz para que se mantenham pessoas capacitadas no compasso em que as mudanças ocorrem.

- O mapeamento das capacidades e os diferentes caminhos possíveis para obtê-las agiliza o processo ensino-aprendizagem e aumenta a efetividade desse processo;
- governança e normativa: a busca do consenso deve ser permanente. Porém, observa-se que dada a multiplicidade de atores, com interesses e motivações legítimos, mas nem sempre convergentes, impõem a definição de responsabilidades e níveis de autoridades compatíveis para que decisões sejam tomadas. Isto foi o que se observou em relação à governança do Setor. Neste contexto, inserem-se as normativas, não apenas para formalizar os processos do sistema, mas para conferir segurança jurídica a ações necessária na defesa do Estado;
- planejamento e execução tempestivos: a mutabilidade já abordada, juntamente com a velocidade de alteração de cenários, impacta decisivamente nos planejamentos. Há que se ter flexibilidade ao executar e prever que planejamentos aderentes à realidade do presente poderão ser inócuos se não executados no tempo adequado. Na cibernética, prever revisões e as consequentes alterações de planejamento no horizonte de cinco anos parece ser coerente com o que a experiência tem mostrado;
- inserção política: a cibernética é eminentemente tecnologia no estado da arte. O viés técnico, inerente da atividade, funciona como catalizador de discussões e atividades. Identifica-se, portanto, uma tendência em limitar abordagens ao nível técnico, em detrimento de níveis de gestão e governança. Como consequência, a inserção política quando ocorre é resultado de situações que já aconteceram, numa abordagem reativa. Por esses motivos, é fundamental que se eleve o tema aos níveis político e estratégico a fim de conquistar uma postura proativa do setor, conferindo a devida prioridade e importância atribuída pelo Estado, frente às ameaças dos cenários do presente e do futuro;
- soluções complexas: as questões na cibernética não são triviais. A citada transversalidade e mudança constante, além do ambiente volátil, sistemas na fronteira do conhecimento e muito mais que se poderia citar para caracterizar o setor geram demandas complexas, cujas soluções não são simples;
- ambiente colaborativo: a cibernética é um fator redutor de assimetrias. Esta não é uma conclusão inédita. Particularmente os que conduzem operações reais atestam quanto dano o mais fraco pode impor ao mais forte até que se chegue a uma resposta adequada. Por este motivo e por tudo o mais que foi apresentado, a colaboração entre integrantes do ecossistema talvez seja a arma

mais eficaz com potencial para mitigar danos e evitar efeitos importantes à segurança e à defesa do Estado.

Ainda que a experiência brasileira na implantação de seu Setor Cibernético de Defesa não tenha trazido ensinamentos inéditos, serviu para confirmar conclusões já vivenciadas por outros países e já, inclusive, mencionadas na literatura disponível.

Buscou-se, portanto, registrar aspectos julgados relevantes na implementação e consolidação do Setor Cibernético de Defesa Brasileiro, onde o Comando de Defesa Cibernética é o órgão central. Embora sejam lições aprendidas e melhores práticas observadas num caso específico, julga-se a pertinência e validade para outros atores. Neste sentido, a intenção é que o conteúdo apresentado seja útil, em alguma medida, para parceiros do ecossistema e que, desta maneira, contribua para o fortalecimento de relações estabelecidas.

General de Brigada Tomás Ramón Moyano egresó del Colegio Militar de la Nación como Subteniente del Arma de Infantería. Por resolución del Presidente de la Nación, fue promovido al grado de General de Brigada. Es Egresado del CHDS (Center for Hemisferic Defense Studies - Washington DC) - Curso de Estrategia y Políticas de Defensa. Agregado Militar Adjunto a la Embajada Argentina en los EEUU de Norteamérica. Comandante de la Xma Brigada Mecanizada "Tte Grl NICOLAS LEVALLE". Actualmente es el Comandante Conjunto de Ciberdefensa.

LA REPÚBLICA ARGENTINA Y SUS ESFUERZOS EN CIBERDEFENSA
EL COMPROMISO CON LAS BUENAS PRÁCTICAS COMO PARTE DE SU IDEARIO

> "El propio concepto de "Buena Práctica" otorga una validación que destaca e institucionaliza propiedades y cualidades que hacen a una práctica buena más allá de su contexto específico. El reconocimiento de una Buena Práctica lleva implícito el de su transferibilidad, dado que se la entiende susceptible de convertirse en referencia para la acción en otras situaciones similares. Es necesario considerar sin embargo que una práctica no sólo es buena porque es eficaz y eficiente sino porque lleva incorporados valores que se consideran positivos, en este sentido las prácticas nunca son neutras…"
>
> Extraído de: Reflexiones en torno al Intercambio de Buenas Prácticas
> El Ágora – Asociación Civil sin fines de lucro

I. Introducción

1. Creación del Comando Conjunto de Ciberdefensa. Pilares organizacionales

En el marco de la transformación que ha experimentado el conflicto en el contexto internacional y los desafíos que este aspecto plantea en materia de Defensa, la República Argentina vio como necesario asumir el compromiso de preparar a sus Fuerzas Armadas para este nuevo escenario. Las acciones liminares a la creación del Comando Conjunto de Ciberdefensa las podemos representar en una sucesión cronológica, materializada en distintos documentos hasta mayo de 2014, momento de su creación. Posterior a ese año otros documentos fueron complementando o adecuando la nueva organización creada.

La consideración del ciberespacio como una dimensión operacional utilizada por el hombre con distintos fines, que puede derivar en situaciones de tensión, crisis y conflicto y la adecuación del Sistema de Defensa Nacional a las nuevas variables del conflicto, sumado a la característica de no ser propia de un ámbito específico, dio origen a la creación del Comando Conjunto de Ciberdefensa (en adelante CCCD) para garantizar la defensa de aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar y aquellos dirigidos a afectar los Objetivos de Valor Estratégico que se determinen para su protección.

Con los documentos rectores que establecen las bases fundacionales del CCCD, se dio inicio a la ardua tarea organizacional con un grupo destacado, pero a la vez reducido de personas. Sobre ellos recayó la responsabilidad de redactar los postulados que fijan la impronta de esta joven, dinámica y cada vez más experimentada estructura. Como es propio de aquellas organizaciones destinadas a evolucionar en el tiempo, se puso énfasis en aquellos aspectos trascendentes que no van a cambiar y que van a acompañar al CCCD en su tránsito al futuro. En este marco se redactó la Visión, como *leitmotiv* de sus integrantes y los Valores que sustentan a la organización, los cuales una vez internalizados en cada uno de sus miembros, representan un *intangible* que trasciende a la organización de la que forma parte.

COMANDO CONJUNTO DE CIBERDEFENSA

Visión

El Comando Conjunto de Ciberdefensa aspira a constituirse como la máxima instancia militar de coordinación del Estado Mayor Conjunto de las Fuerzas Armadas de la Nación, con el fin de alcanzar solidaria y armónicamente los objetivos que se determinasen, en un entorno caracterizado por la disciplina, la discreción y la vocación de servicio.

Valores

- Ética
- Lealtad
- Discreción
- Disciplina
- Vocación de Servicio
- Excelencia profesional
- Alegría
- Armonía
- Trabajo en Equipo

Guiada por la Visión y coherente con los Valores expresados, el CCCD materializa sus acciones a partir de una Misión, clara y definida, otorgando de esta manera a sus integrantes fronteras dentro de las cuales poder desarrollarse.

Misión

Ejercer la Conducción de las Operaciones de Ciberdefensa en forma permanente a los efectos de garantizar las Operaciones Militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el Planeamiento Estratégico Militar.

Conforme a la evolución que ha evidenciado la ciberdefensa en la República Argentina desde el 2010 hasta la fecha, se ha conformado una estructura que ha trascendido el ámbito del Sistema de Defensa Nacional, pero en el cual el CCCD participa activamente. Dentro de esa estructura y a través de distintas relaciones o vinculaciones, desarrolla las actividades que le son propias, manteniendo como premisa fundamental excluyente el ejercicio de las Buenas Prácticas.

2. El Sistema de Ciberseguridad de la República Argentina

El plexo legal de la República Argentina tiene diferenciados los ámbitos de Defensa y Seguridad a partir de la ley Nro 23.554 - Defensa Nacional y la ley Nro 24.059 – Seguridad Interior. Excepto en las circunstancias excepcionales que establecen las normas citadas y algunas ampliaciones realizadas en 2018 por Decretos Presidenciales, las Fuerzas Armadas no poseen atribución para involucrarse en aspectos que sucedan en el ámbito de la Seguridad Interior. Tal situación aplica a la protección cibernética. En este marco referencial, la ciberdefensa en la República Argentina forma parte de un sistema mayor constituido por otros organismos del Estado, que adecuadamente integrados permiten a la Nación el ejercicio pleno de su soberanía. A fin de lograr una adecuada interpretación del Sistema en el cual está inscripto el CCCD, se presenta a continuación un esquema del mismo.

Esquema del Sistema Nacional de Ciberseguridad. Fuente: elaboración propia del CCCD

El ápice del Sistema Nacional de Ciberseguridad está materializado por el Comité de Ciberseguridad, creado por Decreto del Presidente de la Nación Argentina Nro 577/17. Posteriormente esa norma jurídica fue actualizada y ampliada por el Decreto 480/2019, el cual en su Art 1º expresa:

"Créase el COMITÉ DE CIBERSEGURIDAD en la órbita de la SECRETARÍA DE GOBIERNO DE MODERNIZACIÓN de la JEFATURA DE GABINETE DE MINISTROS, el que estará integrado por representantes de la citada Secretaría de Gobierno, de la SECRETARÍA DE ASUNTOS ESTRATÉGICOS de la JEFATURA DE GABINETE DE MINISTROS, del MINISTERIO DE DEFENSA, del MINISTERIO DE SEGURIDAD, del MINISTERIO DE RELACIONES EXTERIORES Y CULTO y del MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS, el cual tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad.

El COMITÉ DE CIBERSEGURIDAD, será presidido por el Secretario de Gobierno de Modernización, en su carácter de Vicejefe de Gabinete de la JEFATURA DE GABINETE DE MINISTRO[1]

[1] Boletín Oficial de la República Argentina No. N 49.980/19 del 12 Jul 19. Consultado en su versión en línea el 05 Oct 19.

El Comité de Ciberseguridad surge como una respuesta a la necesidad de reunir a los representantes de las principales áreas de gobierno vinculadas a la problemática del ciberespacio para elaborar la Estrategia Nacional de Ciberseguridad y, una vez aprobada esta, desarrollar el plan de acción necesario para la implementación de dicha Estrategia. Es conveniente aclarar que a pesar de que los ámbitos de actuación en el ciberespacio están divididos en Ciberseguridad y Ciberdefensa, cuando hablamos de Ciberseguridad en términos de políticas o estrategias, nos referimos a un concepto sobre la situación en la cual una Infraestructura Crítica se considera protegida de amenazas o agresiones cibernéticas, proporcionando libertad de acción para el empleo de dicha infraestructura, de acuerdo a los lineamientos establecidos en la Estrategia Nacional de Ciberseguridad.

En el ámbito de la ciberdefensa propiamente dicha, mediante Decreto del Presidente de la Nación Nro 42/2016 del 07 Ene 16, se crea en la órbita del Ministerio de Defensa, la Subsecretaría de Ciberdefensa, dependiente de la Secretaría de Estrategia y Asuntos Militares, con Control Funcional sobre el Comando Conjunto de Ciberdefensa.

Como se puede apreciar, la multiplicidad de actores involucrados en la problemática de la Ciberseguridad, la actualización de normas, la ampliación de atribuciones, entre otros aspectos, da cuenta de la dinámica que presenta el ciberespacio como nuevo ámbito de operaciones. Para desenvolverse en él, el CCCD considera que adquiere particular relevancia en su accionar las "Buenas Prácticas", las cuales proporcionarán legitimidad a sus actos, convirtiéndose de esta manera en una eficaz herramienta del Estado para hacer frente a este nuevo escenario del conflicto.

II. Desarrollo

1. El Comando Conjunto de Ciberdefensa y la materialización de las Buenas Prácticas

A fin de poder enmarcar las acciones del CCCD en las Buenas Prácticas, hemos tomado como Marco Teórico las "Buenas Prácticas en la Estrategia Nacional de Ciberseguridad" que ofrece la "Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad"[2] buscando trazar una relación de correspondencia entre lo descripto en ese documento y el accionar del CCCD, observando que algunas de las Esferas de Interés consideradas en las Buenas Prácticas han sido debidamente desarrolladas por este Comando. Si bien la Guía de referencia apela a un trabajo

[2] La Unión Internacional de Telecomunicaciones (UIT), el Banco Mundial, la Secretaría de la Commonwealth (Comsec), la Organización de Telecomunicaciones de la Commonwealth (CTO), el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE OTAN). 2018. *"Guía para la elaboración de una estrategia nacional de ciberseguridad – Participación estratégica en la ciberseguridad"*. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO).

integral como es el desarrollo de una Estrategia Nacional de Ciberseguridad, también las Esferas de Interés pueden ser aplicadas a una escala menor (el CCCD), para alcanzar los propios objetivos y prioridades de acuerdo con la Visión, Valores y Misión.

A continuación, se desarrolla el siguiente esquema para graficar las siete Esferas de Interés:

Esquema de las Esferas de Interés de las Buenas Prácticas. Fuente: elaboración propia del CCDD

Seguidamente se describirán aquellas Esferas de Interés, asociadas a las Buenas Prácticas en las que mayor injerencia tiene el CCCD.

a. Cooperación Internacional

Desde su creación el CCCD ha buscado relacionarse internacionalmente con aquellos países de mayor trayectoria y experiencia en ciberdefensa y con otros países con los cuales, por poseer experiencia similar a la nuestra y por formar parte del marco regional, interesa vincularse. En este sentido este Comando sostiene tres tipos de relacionamientos, el primer tipo: Recibimiento de Autoridades, a través de visitas de militares o autoridades extranjeras al CCCD, el segundo tipo: Relaciones Bilaterales, a través de Intercambios de Personal, Reuniones Bilaterales, Ejercicios y Cursos. Tal es el caso de las experiencias realizadas con BRASIL, CHILE, COLOMBIA, ITALIA, JAPÓN, PERÚ, ESPAÑA, ALEMANIA, ISRAEL y ESTADOS UNIDOS. El tercer tipo de

relacionamiento es a través del Foro Iberoamericano de Ciberdefensa. La iniciativa del Foro surge como una impronta del Reino de España firmando una Carta de Intenciones en mayo de 2016 inicialmente ocho países (ARGENTINA – BRASIL – CHILE – COLOMBIA – ESPAÑA – MÉXICO – PERÚ – PORTUGAL) posteriormente solicitaron su incorporación al Foro URUGUAY y PARAGUAY, sumando a la fecha diez países. El objeto del foro fue promover la colaboración en ciberdefensa entre las Fuerzas Armadas de los países miembros en las áreas de formación, ejercicios, intercambios de información, investigación, desarrollo e innovación, en el ámbito del ciberespacio como otro dominio inherente a la Defensa Nacional y por lo tanto motivo de análisis, estudio, formación y adiestramiento por parte de las Fuerzas Armadas. En atención al espíritu con que fue creado, en octubre de 2017 se desarrolló en Brasilia el Ier Ejercicio Iberoamericano de Ciberdefensa. En dicha oportunidad se propuso a la República Argentina como país sede del II^{do} Foro Iberoamericano de Ciberdefensa, a fin de continuar los esfuerzos de cooperación para alcanzar los objetivos comunes trazados, fortaleciendo las relaciones existentes.

Entre el 20 y 22 de marzo de 2018 año se desarrolló en Buenos Aires el II^{do} Foro Iberoamericano de Ciberdefensa (FIC) organizado íntegramente por el CCCD, donde además de los representantes de los Estados miembros se invitó a representantes de los países de la región interesados en la problemática. Asimismo, participaron autoridades militares del Estado Mayor Conjunto de las Fuerzas Armadas, del Ejército, Armada y Fuerza Aérea, autoridades del ámbito académico y de distintas áreas de Gobierno. Durante el desarrollo se dieron exposiciones por parte de las diferentes Delegaciones asistentes al evento, donde se reflejaba la problemática de cada país y la manera como abordaban a la solución. Como resultado de las intensas jornadas se firmó una Carta de Intenciones cuyos puntos salientes fueron:

1) Desarrollar durante el mes de marzo de cada año el FIC, en aquellos países que sean designados sede y durante el mes de octubre de cada año se desarrollará el Ejercicio de Ciberdefensa.

2) Designar al país que se desempeñe como Sede del FIC, como Secretaría Pro Tempore y responsable de la carga administrativa que devenga hasta el siguiente Foro.

3) Trabajar para el establecimiento de un protocolo de cooperación para la difusión de avisos, alertas y alarmas de ciberataques.

4) Trabajar en la creación y aplicación de una MISP (Malware Information Sharing Platform), para intercambio de información entre países iberoamericanos.

5) Brindar apoyo entre países amigos para grandes eventos.

6) Evolución de la Carta de Intenciones del FIC.

7) Evaluar posibilidades de colaboración en actividades de educación y entrenamiento (cursos).

A su vez se dejó plasmado en dicho documento el procedimiento para la incorporación de nuevos países que pretendan incorporarse al FIC. Asimismo, Portugal asumió la responsabilidad de redactar las normas que regirán tanto la organización de los próximos Foros como así también las pautas que regulan el desarrollo de los ciberejercicios, las cuales fueron aprobadas durante el III^{er} FIC. También se propuso integrar al FIC a la República Oriental del Uruguay, para lo cual y conforme al procedimiento establecido y a las comunicaciones efectuadas por la Secretaria del Foro, se aprobó de manera unánime su inclusión.

El 30 de agosto de 2018, en el marco de las Ciberolimpiadas organizadas por Colombia, en su Etapa On Line el CCCD obtuvo el 3er Puesto entre trece países, lo que permitió que este Comando, en representación de las Fuerzas Armadas de la República Argentina, participara en la Etapa Presencial de ese importante evento. Para tal ocasión el personal seleccionado viajó a Bogotá - Colombia en noviembre de 2018, donde participó a lo largo de tres jornadas de las Ciberolimpiadas.

Entre el 22 y 25 de octubre de 2018 un Equipo integrado por personal del CCCD, personal de la Dirección de Ciberdefensa del Ejército y personal de la Dirección de Ciberdefensa de la Fuerza Aérea, participaron del 2do Ejercicio del Foro Iberoamericano de Ciberdefensa, que tuvo lugar en España, en la Base de Retamares, sede del Mando Conjunto de Ciberdefensa español (MCCD). Los objetivos del ejercicio se elaboraron según las Normas para el Funcionamiento del Ejercicio a desarrollarse en el marco del Foro Iberoamericano de Ciberdefensa fueron:

1) Fomentar la cooperación entre los países pertenecientes al Foro Iberoamericano de Ciberdefensa en este ámbito, sin espíritu de competición.

2) Mejorar la preparación para conducir un Ejercicio Internacional en el marco del Foro Iberoamericano de Ciberdefensa.

3) Entrenar las capacidades técnicas cibernéticas de los equipos involucrados en la actividad.

4) Identificar las posibilidades para realizar intercambio de información.

5) Fomentar el establecimiento del protocolo de cooperación para la difusión de avisos, alertas y alarmas de ataques cibernéticos, conforme consta en la Carta de Intención del II Foro Iberoamericano de Ciberdefensa.

6) Fomentar la creación de una plataforma electrónica de intercambio de información de malware (MISP), para intercambio de información entre los países Iberoamericanos, conforme consta en la Carta de Intención del II Foro Iberoamericano de Ciberdefensa.

7) Incrementar el conocimiento mutuo de las doctrinas de empleo en el espacio cibernético.

Conforme a las propuestas efectuadas, el FIC 2019 se desarrolló en Brasil y el Ciberejercicio en su tercera edición también tendrá a ese país como Sede.

De la Carta de Intenciones suscripta por los representantes de los países miembros, los puntos más salientes fueron:

1) Elaborar de un “Marco de Referencia Doctrinario del Ciberespacio”, que defina el rol de las Fuerzas Armadas y su marco de actuación general; y que incluya, además, un glosario de términos unificado en la materia.

2) Estudiar la posibilidad de compartir información, bilateralmente, acerca los siguientes asuntos:

a) La forma en que están desarrollando operaciones ofensivas, cuál es el proceso y si hay un marco jurídico que respalde estas acciones.

b) Difusión de doctrina conjunta, combinada y multilateral con aliados para el desarrollo de operaciones cibernéticas.

c) Plan de carrera para los cibercomandos y qué estrategias existen para retener el capital intelectual humano capacitado.

d) La forma en que están generando doctrina conjunta para ciberdefensa.

3) El III Ejercicio Iberoamericano de Ciberdefensa definirá como objetivo integrar y fortalecer la cooperación entre países miembros para reaccionar ante un ataque cibernético con

capacidad de respuesta. Se propuso incluir en el objetivo del III Ejercicio Iberoamericano de Ciberdefensa la integración del Planeamiento de Ciberoperaciones en apoyo a las Operaciones de mar, aire y tierra, a fin de continuar generando doctrina en este rubro.

4) Llevar a cabo los desarrollos y gestiones necesarios para implementar, en todos los países miembros integrantes del Foro Iberoamericano, bases integradas en la plataforma MISP. (Dicha intención ya se materializó).

5) Efectuar sesiones virtuales con los representantes de los países miembros cada 3 meses para dar a conocer buenas prácticas, lecciones aprendidas y casos emblemáticos en cada uno de los países, para compartir con los demás. (Dicha intención se viene cumplimentando de manera periódica a través de videoconferencias).

b. Legislación y Reglamentación

En esta Esfera de Interés, la promulgación de la Legislación respectiva por parte de las distintas carteras ministeriales, como así también las necesidades que surgen para incorporar la ciberdefensa al planeamiento y ejecución de las operaciones que realiza el Instrumento Militar, proporcionan el *input* para que el CCCD se aboque a la elaboración de la doctrina necesaria para el adecuado empleo de los medios de ciberdefensa a disposición. La doctrina de ciberdefensa elaborada en el ámbito del Estado Mayor Conjunto de las Fuerzas Armadas (denominada Doctrina Conjunta), sirve de base para la elaboración de la doctrina propia, por parte de cada una de las organizaciones de ciberdefensa de las Fuerzas Armadas (denominada Doctrina Específica). De esta manera y desde el punto de vista de la ciberdefensa, el circuito doctrinario queda debidamente articulado para todo el Instrumento Militar. A su vez, personal del CCCD con amplia formación y experiencia participa en equipos *Ad Hoc* para la actualización doctrinaria, asesorando sobre aquellos conceptos de ciberdefensa que son necesarios incorporar en los diferentes reglamentos.

Vinculado con la Cooperación Internacional, a partir de acuerdos bilaterales que el Estado Mayor Conjunto de las Fuerzas Armadas suscribe con países amigos, se ha avanzado en la elaboración de Doctrina de Ciberdefensa Combinada en un paso más para lograr el adecuado entendimiento y avanzar en la aplicación de las Buenas Prácticas de la Ciberdefensa en la ejecución de Operaciones Combinadas.

c. Capacitación, Creación de Competencias y Sensibilización

1) Plan de Formación en Ciberdefensa

En esta esfera de Interés, el CCCD ha trabajado bajo la consideración de que la construcción de una ciberdefensa eficaz y eficiente no sólo contribuye a mejorar en su conjunto la Seguridad de la Información del Instrumento Militar, sino que, como factor de disuasión, es un objetivo irrenunciable que depende en gran medida de la calidad de la formación de todos cuantos tienen alguna responsabilidad directa en la materia. La consecución de este objetivo debe basarse en la definición, implementación y continuo perfeccionamiento de una formación orientada hacia las funciones de cada uno de los puestos directamente relacionados con actividades de ciberdefensa, tanto en la conducción de Operaciones del Ciberespacio como en los aspectos técnicos y eminentemente operativos. En ese sentido, es necesario alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita el Instrumento Militar para sustentar todos los objetivos de Ciberdefensa.

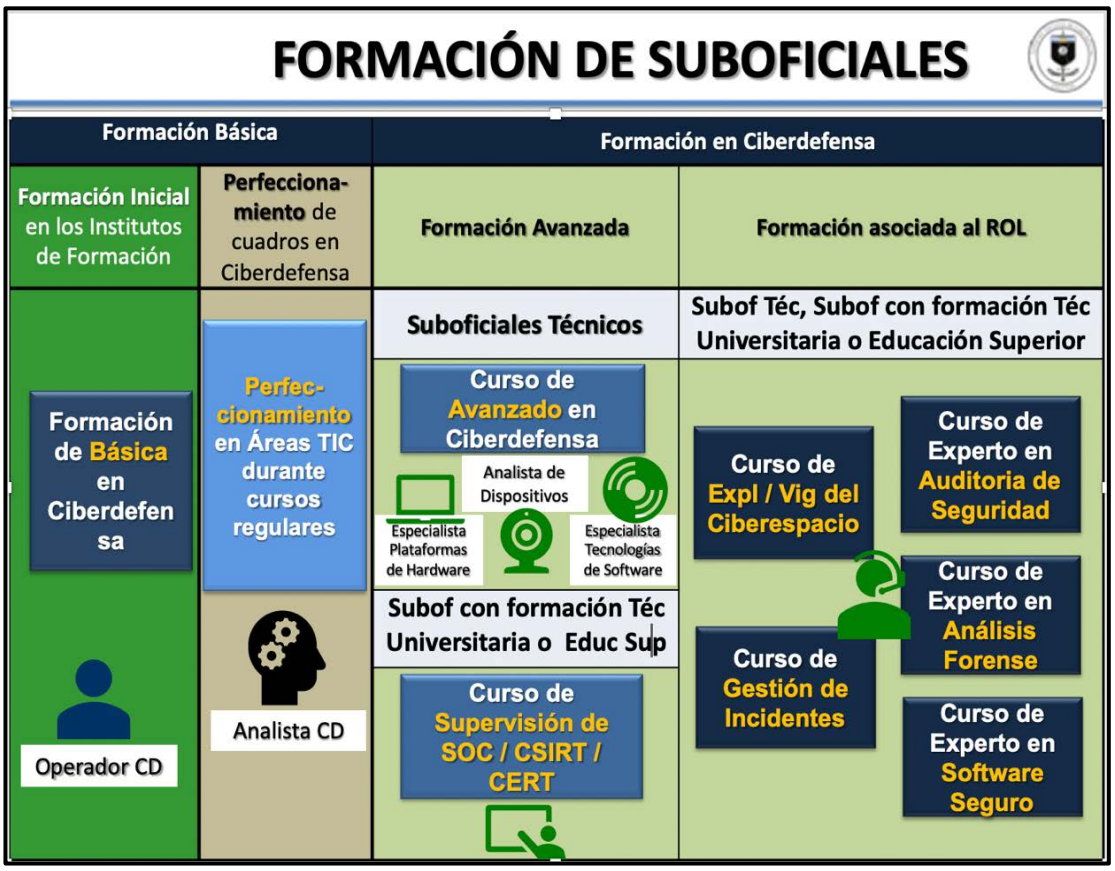
Conforme a lo expresado precedentemente, el Comando Conjunto de Ciberdefensa asumió la responsabilidad de definir, dirigir y coordinar la concientización, la formación y el adiestramiento especializado en materia de ciberdefensa. Del estudio de los cometidos relacionados con la ciberdefensa y de las necesidades formativas que de todo ello se derivan, el Comando Conjunto de Ciberdefensa ha desarrollado un Plan de Formación en Ciberdefensa, que será el instrumento para la adquisición, mejora y actualización de competencias necesarias en aspectos relativos a la ciberdefensa. Este plan facilita, además, la implementación de los trayectos formativos que permitirán alcanzar la capacitación necesaria a cada uno de los distintos grupos de formación identificados.

Un análisis de la situación ha permitido determinar que, en la actualidad, la formación en este ámbito es escasa, parcialmente satisfecha con perfiles técnicos del área TIC, sin conocimientos profundos de las Operaciones Militares ni de Operaciones del Ciberespacio, no está debidamente estructurada ni homologada, y no garantiza la capacitación del personal para el acceso a formación de mayor nivel tecnológico ni para satisfacer las necesidades reales de las FF AA en la Conducción de Ciberoperaciones. No obstante, se considera que la formación en ciberdefensa se debe apoyar en gran medida en los activos de las FF AA y se acreditarán mediante títulos o certificados obtenidos de la forma que se determine para cada caso.

El Plan fue concebido con el objetivo fundamental de definir los requisitos de formación basados en perfiles, en materia de ciberdefensa, que deberían alcanzar los integrantes de las FFAA que ocupen puestos de trabajo relacionados con la ciberdefensa. Será también de aplicación tanto para el personal militar como para el personal civil que se incorpore a las organizaciones de Ciberdefensa. A su vez, este Plan persigue como finalidad la descripción de las responsabilidades generales en formación de ciberdefensa en el ámbito de las FF AA. En este sentido, y a futuro, los programas de formación y los planes de estudio de los Institutos Militares en donde se desarrolle la formación en ciberdefensa deberán tener en consideración el presente Plan. En su diseño se ha contemplado, en el mayor grado posible, el aprovechamiento de las estructuras de los Planes de Carreras vigentes en las FF AA. De igual manera, se definen también los mecanismos para la actualización continua en las competencias del personal.

El proceso de evaluación de este plan se llevará a cabo de acuerdo con las normas de evaluación del sistema de enseñanza militar, de manera progresiva, con el propósito de que se encuentre completamente implementado en el corto plazo. El análisis y estudio de los resultados de este plan servirán de base para los futuros reajustes. Dentro del presente documento se establecen dos partes diferenciadas, una primera relacionada con la identificación de los grupos funcionales del personal relacionado de alguna forma con la ciberdefensa y sus necesidades formativas, y una segunda relacionada con la mejora y adaptación de este Plan.

Esquema del Plan de Formación de Oficiales. Fuente: elaboración propia del CCCD



Esquema del Plan de Formación de Suboficiales. Fuente: elaboración propia del CCCD

2) Plan de Concientización y Sensibilización.

Por similitud a lo que sucede en otras áreas, se puede afirmar que en Ciberseguridad el eslabón más débil es el individuo como usuario del sistema. A su vez, si se considera que la innovación y avance tecnológico son continuos y aventajan, en algunos casos, la capacidad de adopción de medidas de seguridad, resulta entonces necesario implicar activamente a todos los usuarios en la protección y defensa de las redes y de los sistemas de información vinculados a las FFAA. En este sentido, se debe tener presente que la gestión eficaz de los riesgos derivados del ciberespacio debe edificarse sobre una sólida cultura de Ciberseguridad. Ello requiere de los usuarios una comprensión particular respecto de los riesgos que existen al operar en este medio, así como del conocimiento de las herramientas para la protección de su información, sistemas y servicios.

La instalación en la conciencia del personal de las FF AA de una sólida cultura de Ciberseguridad proporcionará a todos los actores la responsabilidad y la confianza necesaria para su interacción en un medio tan complejo y sensible como es el del ciberespacio. El CCCD se impuso como responsabilidad la de *"Especificar, coordinar la concientización, formación y el adiestramiento especializado en materia de Ciberdefensa para el Personal integrante de las FFAA"*, definiendo a la concientización como las acciones necesarias para facilitar al personal la compresión de las amenazas generadas por los potenciales adversarios o elementos hostiles en el ciberespacio; así como la manera en la que, tanto a nivel individual como colectivo, se puede y debe contribuir a evitar o contrarrestar estas amenazas, reaccionando oportuna y adecuadamente. Al respecto se debe dejar establecido que la seguridad de la información es responsabilidad de todos los miembros de las Fuerzas Armadas, los cuales deberán estar adecuadamente formados y concientizados para el satisfactorio cumplimiento de sus responsabilidades.

A fin de contribuir a la toma de conciencia del personal, el CCCD elaboró un **Plan de Concientización de Ciberdefensa para el Personal de las Fuerzas Armadas**, el mismo tiene por finalidad, definir un conjunto de acciones dirigidas a todos los usuarios de las Tecnologías de la información y la comunicación (TIC), integrantes de las FFAA, para que sean conscientes de los riesgos y amenazas a los que diariamente se enfrentan en el ciberespacio, así como la forma de prevenir, atenuar y mitigar sus efectos. Como aspecto secundario se persigue la extensión de éstas acciones a su ambiente familiar, con independencia a que su puesto de trabajo implique o no el uso de las TIC, toda vez que este personal es susceptible de hacer uso de éstas en otros ámbitos, con impacto posible en el entorno de las FF AA. A su vez el Plan describe las responsabilidades generales de la concientización en el marco de las FFAA y los recursos necesarios para su implementación.

Nro	Líneas de concientización	Objetivos generales de concientización	
1	General	1.1	Dar a conocer los riesgos del ciberespacio.
		1.2	Informar que las FFAA son objetivo de ciberataques, aumentando esta circunstancia el nivel de amenaza al que está sometido su personal.
2	Identificación y credenciales de acceso	2.1	Concientizar de la importancia de una gestión adecuada de las contraseñas y de otras credenciales de acceso en la protección de la información.
3	Navegación por Internet	3.1	Promocionar el uso responsable de Internet.
		3.2	Difundir hábitos y buenas prácticas de navegación por Internet.
		3.3	Enseñar cómo identificar enlaces potencialmente peligrosos.
		3.4	Recomendaciones específicas para el uso de servicios electrónicos homebanking y pagos on-line.
4	Correo electrónico	4.1	Advertir que el correo electrónico es uno de los medios más frecuentes de ciberataque, puesto que no es un método totalmente seguro para intercambiar información fuera del ámbito de las FFAA.
		4.2	Enseñar cómo identificar mensajes potencialmente peligrosos ("phising" y fraudes on-line).
5	Servicios en la red	5.1	Difundir recomendaciones de uso seguro de servicios en internet, conciliando la productividad con la seguridad.
		5.2	Recomendaciones específicas para proteger la información personal en Internet.
6	Actividad en redes sociales	6.1	Explicar a los usuarios cómo pueden ser víctimas de ataques de "ingeniería social", especialmente en las redes sociales.
		6.2	Promover la prudencia en el uso de las redes sociales, especialmente a la hora de publicar información.
		6.3	Prevenir situaciones de riesgo para las FFAA o terceras personas que tienen relación con los usuarios.
7	USB y soportes de información	7.1	Avisar de los riesgos asociados al uso de soportes y dispositivos de almacenamiento USB (infección, pérdida de información y posible infracción de la normativa).
8	Protección del entorno personal	8.1	Explicar a los usuarios cómo pueden proteger su PC personal.
		8.2	Enseñar cómo es posible trasladar esta protección a los dispositivos y redes personales en el ámbito personal.
9	Fuera de la oficina: Movilidad	9.1	Informar a los usuarios de su especial vulnerabilidad en situación de movilidad fuera de su puesto de trabajo.
		9.2	Explicar a los usuarios cómo pueden proteger los dispositivos móviles y portátiles tanto en el ámbito profesional como en el personal.
10	Prevención y reacción ante los incidentes	10.1	Poner de manifiesto la importancia de la participación de los usuarios en la detección temprana y respuesta a incidentes de ciberseguridad.
		10.2	Fomentar que el usuario acuda a informarse sobre los riesgos y alertas de seguridad a través de los portales falsos.
		10.3	Enseñar a identificar incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
		10.4	Difundir el procedimiento para comunicar incidencias de seguridad, sean reales o falsas alarmas a las unidades encargadas de gestionarlas.

Ejemplo de Líneas de Concientización y Objetivos perseguidos del Plan de Concientización en Ciberdefensa. Fuente: elaboración propia del CCCD

d. Gestión de Riesgos para la Ciberdefensa / Preparación y Resiliencia.

El CCCD ha confeccionado bajo un enfoque sistémico, un manual de procedimientos estandarizados, los que pueden considerarse como actividades de procesos y subprocesos de ciberdefensa Pasiva. Se enfocan principalmente en la descripción de los Procedimientos Operativos Normales destinados a ejecutar la Defensa Pasiva de Infraestructuras Críticas de la Información del Instrumento Militar (Sistemas de Comando y Control, Sistemas de Comunicaciones, Sistemas de Armas, Sistemas de Control, Sistemas Computarizados en apoyo a las Operaciones Militares) y otros Recursos Esenciales de Sistemas, Redes, Datos e Información de las FFAA, siendo de aplicación en tiempo de paz para adiestrar, entrenar y ejecutar las acciones del Sistema de Respuesta de Ciberdefensa por parte del Centro de Operaciones de Ciberdefensa del CCCD principalmente. El Manual de Procedimientos fue difundido a las FF AA para su implementación como así también para la incorporación de mejoras, conforme a las Lecciones Aprendidas de la Experiencia de cada organización, dado que las amenazas a la Ciberseguridad se presentan tan dinámicas como impredecibles, cualquier procedimiento que se instaure, requiere una actualización constante.

Ejemplo de Procesos y Subprocesos del Manual de Procedimientos del CCCD.
Fuente: elaboración propia del CCCD

Ejemplo de Procesos y Subprocesos del Manual de Procedimientos del CCCD. Fuente: elaboración propia del CCCD

e. Servicios de Infraestructura Fundamental y Servicios Esenciales.

Conforme a la Misión impuesta, el CCCD debe estar en capacidad de repeler aquellos ciberataques contra las Infraestructuras Críticas de la Información y las Comunicaciones y los activos del Sistema de Defensa Nacional[3] y del Instrumento Militar. No obstante, la Directiva Política de Defensa Nacional 2018 establece:

1) Relacionado a Amenazas Cibernéticas:

"…El abordaje de esta problemática desde la perspectiva de la Defensa Nacional requiere adoptar medidas y acciones tendientes a resguardar la seguridad cibernética de las infraestructuras críticas del Sistema de Defensa Nacional ***y de aquellas que sean designadas para su preservación, independientemente del origen de la agresión…"***

[3] El Sistema de Defensa Nacional se encuentra definido en el Art 9 de la Ley 23.554 - Defensa Nacional.

2) Relacionado a Riesgos

a) Ataques externos a Objetivos Estratégicos:

> *…El Sistema de Defensa Nacional debe planificar y proteger los objetivos estratégicos que puedan ser objeto de una agresión de origen externo. […]* ***La atención de este riesgo debe focalizarse particularmente en aquellas infraestructuras cuyo funcionamiento resulte crítico para el cumplimiento de las funciones vitales del Estado Nacional, su Defensa Nacional, el ejercicio de la soberanía y el resguardo de la vida y la libertad de sus habitantes."***

Considerando los dos aspectos referidos, será responsabilidad del CCCD, planificar la protección cibernética de aquella Infraestructura Crítica y/u Objetivos Estratégicos, alguno de los cuales prestarán un servicio esencial a la Nación. En esa planificación adquirirá un valor especial las vinculaciones con todos aquellos estamentos del Estado, necesarios para lograr las coordinaciones a fin de evitar superposiciones en el esfuerzo que demande la protección. Asimismo, debe contemplarse un estrecho relacionamiento con el ámbito privado, ya que muchos de los servicios esenciales del país están en manos de ese sector. En tal sentido, el ejercicio de las Buenas Prácticas y fundamentalmente los antecedentes que se tengan de su correcta implementación en otras Esferas de Interés, serán de particular importancia ya que operarán como un catalizador para generar los lazos de confianza necesarios para la eficiente y eficaz ciberdefensa del objetivo que se trate.

III. Conclusiones

Los distintos Estados han buscado enfrentar las amenazas y riegos que implica el ciberespacio y que afectan a los conceptos de seguridad y defensa de diferentes maneras pero que básicamente responde, entre otros aspectos, a: la conformación de estructuras organizativas que permitan proteger sus activos digitales; la adecuación del marco legal que le permita desenvolverse en ese ambiente marcando los límites que tiene su accionar y penalizando a quienes los infringen; la incorporación de contenidos en sus programas educativos, buscando desde la temprana edad

crear conciencia de los riesgos que acechan en el ciberespacio y facilitando la formación de especialistas; la suscripción de acuerdos internacionales que favorezcan la cooperación de esfuerzos; la creación de estrategias y políticas que permitan alcanzar los objetivos deseados, etc.

Las organizaciones internacionales también se han esforzado en dotar con modelos o estrategias para afrontar las amenazas de ciberdefensa y ciberseguridad de los Estados. Han publicado varios documentos o estándares, como la *Guía de la ciberseguridad para los países en desarrollo* (ITU 2007) o el *National Cybersecurity Strategy Guide* (ITU 2018). Ambos son modelos de referencia basados en la valoración de activos, capacidades, necesidades, amenazas y riesgos en sectores públicos y privados del Estado para construir y ejecutar una estrategia de ciberseguridad nacional. No podemos dejar de hablar de entidades de estandarización como la Organización Internacional de Normalización (ISO), que con sus *Sistemas de Gestión de Seguridad de la Información (SGSI)* contenidas en la ISO/IEC 27000, *Tecnologías para la seguridad de la Información y Técnicas de Seguridad* pretende dar una propuesta más orientada a los aspectos específicos de seguridad en una entidad u organización.

La República Argentina, en la búsqueda de la Ciberseguridad y Ciberdefensa de sus Infraestructuras Críticas, viene realizando esfuerzos que se materializan en el ámbito político, legislativo, judicial, académico y científico tecnológico. La creación del Comando Conjunto de Ciberdefensa es parte de la respuesta, desde el punto de vista de la Defensa, a la problemática que plantea el ciberespacio. A pesar de que, como se expresara en el párrafo precedente, existen modelos integrales para encarar la ciberseguridad y la ciberdefensa, el país no ha logrado adaptarse completamente a alguno de estos modelos.

No obstante, desde su origen, el CCCD ha buscado erigirse como un referente en materia de ciberdefensa, donde el ejercicio de las Buenas Prácticas en todo su accionar responde a los conceptos rectores de su creación. Asimismo, y a partir de las relaciones orgánicas y funcionales otorgadas para su vinculación con las Direcciones de Ciberdefensa de las Fuerzas Armadas, permite trasladar su impronta a ellas. Su relacionamiento internacional, fundamentalmente a través del Foro Iberoamericano de Ciberdefensa como así también la participación en otros espacios de debate, es un intento de intercambiar experiencias y conocimientos que resulten beneficiosos para la organización. En el ámbito de la formación y concientización, se considera que la excelencia en la capacitación de los Recursos Humanos es fundamental. A partir de esa premisa y a través de la elaboración de sendos planes, el CCCD pretende dar un aporte a los decisores que tienen en sus

manos la posibilidad de su implementación y articulación. La gestión de riesgos a partir de la elaboración de un Manual de Procedimientos que se suma a la elaboración de Doctrina Conjunta y Combinada, ha tenido su correlato de éxito en la ciberseguridad y ciberdefensa de grandes eventos, tal como fue la colaboración prestada con miembros del CCCD en el CSIRT del Gobierno de la Ciudad Autónoma de Buenos Aires, durante la realización de los Juegos Olímpicos de la Juventud durante el 2018, como así también durante la ciberdefensa de la Cumbre del G-20, realizada en Buenos Aires en diciembre de 2018. La posibilidad que le otorga la Directiva Política de Defensa Nacional, en los aspectos referidos a Riesgos y Amenazas Cibernéticas, le confieren al CCCD la posibilidad de la planificación de la ciberdefensa de aquellas Infraestructuras Críticas y Objetivos Estratégicos que el Nivel Político le asigne para su protección, en un ambiente tan difuso y sin límites físicos como es el ciberespacio, a lo que se suma la dificultad de la atribución y donde el CCCD deberá articular su accionar con el ámbito público y privado, resulta casi condición *sine qua non* la transparencia y las buenas prácticas.

En el desarrollo del presente trabajo se ha intentado establecer, por analogía, pero a un nivel sensiblemente inferior, utilizando como marco conceptual las Esferas de Interés establecidas en las “Buenas Prácticas en la Estrategia Nacional de Ciberseguridad” que ofrece la “Guía para la Elaboración de una Estrategia Nacional de Ciberseguridad”, aquellos aspectos que ha podido desarrollar el CCCD, en su reducido radio de acción como es la ciberdefensa. Muchos de los aspectos referidos, fueron realizados por iniciativa propia. Es de prever que, a partir de la recientemente promulgada Estrategia de Ciberseguridad Nacional, la expansión del Comité Nacional de Ciberseguridad con la participación de otras carteras ministeriales, la creación de la Dirección Nacional de Ciberseguridad, la definición de términos a partir de un glosario común, sumado a la manera de definir las infraestructuras críticas, impulsarán acciones sobre los distintos actores responsables de la Ciberseguridad/Ciberdefensa, que en el caso particular del CCCD potenciarán el crecimiento de los aspectos ya referidos, en un intento de alcanzar las Capacidades de Ciberdefensa planificadas para el corto, mediano y largo plazo, a fin de proporcionar a la República Argentina de una organización valiosa para la ciberdefensa de sus activos digitales y al Instrumento Militar de un elemento multiplicador de fuerzas. En ese escenario incierto que representa el futuro, el CCCD no abandona un instante el esfuerzo que la tarea le demanda.

Mr. Richard J. Driggers is the deputy assistant director of the Cybersecurity and Infrastructure Agency (CISA) of the Department of Homeland Security. Before being appointed to the Superior Executive Service, he held multiple senior management positions within NPPD and the Office of Intelligence and Analysis. Former Air Force combat controller. He has received multiple awards and military decorations to include the Jumpmaster Parachutist badge, the Military Freefall Jumpmaster badge, the Special Operations combat Diver badge and the Army Ranger tab. He graduated from the Senior Executive Fellows Program at Harvard Kennedy School of Government.

MR. RICHARD J. DRIGGERS SPEECH

CYBERDEFENSE AND SECURITY CONFERENCE

Presentation notes as delivered by Mr. Driggers

I. Introduction

Good Afternoon, thank you Dr. Carneiro for your kind introduction and for inviting me here today.

It is an honor to be here with all of you for a second time this year as we work to deepen the ties between our countries on key cybersecurity issues, including critical infrastructure protection, improving information sharing, and protecting our global supply chains.

While discussing cyber issues can be extensive and varied, it is imperative that we continue to discuss cybersecurity within the context of foreign policy.

Cyberspace threats are not bound by national borders. Our networks and the critical infrastructure they support are integrated into a larger global cyber ecosystem.

Over the past several years, the nature of this threat has evolved and is now more complicated, asymmetric, and much closer to home. Infrastructure – systems that enable our way of life, such as water, transportation, electricity, etc. – continues to be a frequent target of interest by a diverse group of malicious actors – nation-states like Russia, China, Iran and North Korea, as well as cyber criminals, terrorist groups, and others – who can initiate attacks from anywhere in the world.

That being said, as our adversaries become more agile and continue to evolve, so must our collective response, or as we say, collective defense.

That is where my agency, the Cybersecurity and Infrastructure Security Agency (CISA) comes in.

II. What is CISA?

At CISA, we lead the United States government effort to enhance the security, resilience, and reliability of our Nation's cyber and physical infrastructure.

In these efforts, my agency has five immediate priorities we are wrapping our arms around, which include:

- Election security;
- Supply chain risk management, which involves the cyber threats we are seeing from China and the upcoming rollout of 5G technologies;
- Protecting our federal government, or ".gov" networks;
- Soft target security; and
- Critical infrastructure protection, which includes industrial control systems - the processes that provide vital services in critical infrastructure.

While CISA looks at these five priorities and thinks about how to deliver security and resilience, we know we can't do it alone, and we don't want to do it alone.

We recognize that our cyber mission is vast and complex —and too important—for one government agency or even one country to tackle on its own.

We will work across the government, with industry and academia, as well as with our international partners.

III. Supply Chain Risk Management

As the cyber leaders for our respective countries it is important to understand there is a lot of risk out there, and for our purpose we need to prioritize our approach. And nowhere in my view is the risk more apparent than in managing risk in the global cyber supply chain and managing risks associated with the upcoming rollout of 5G technology.

In tackling supply chain challenges, my agency has redoubled its focus on working with the private sector, developers, and international partners to prioritize national security in their decision-making process while initiating partnerships and programs to foster innovation.

We want to get out of being reactive to products that pose real and potential threats and become more proactive by stopping those potentially harmful, overtly vulnerable products from being deployed in the first place.

My agency is especially concerned about the cyber and data risks from information and communications technology (ICT) products designed, developed, manufactured, or supplied by companies operating under the control or influence of a foreign government whose national security interests are adverse to the United States.

We all know there is a certain level of risk with any technology that generates or collects sensitive data, such as industrial control systems. But that risk increases dramatically when the technology comes from a company that could be persuaded or forced to abuse their access on behalf of a foreign government that does not share our Constitutional norms and values or operates without any meaningful checks on its ability to compel cooperation with its intelligence services. The U.S. government has serious concerns about technologies that take American data into the territory of a government that lets – or directs – its intelligence services to open the hood, peek around, and do who knows what with that data.

Those concerns, and that pragmatic worldview, are what led us to develop the framework that I want to share with you today. When we look at supply chain risk management in the context of procurement or acquisition for our nation's supply chain, we are looking at three interconnecting pieces: the what, the where, and the who.

- **First, the what.** For this, we are looking at the technical aspect of a product or service. In doing so, we are examining a variety of concerns. For example, we want to identify what functions the product or service performs and how it operates; whether the product receives software updates from the supplier; and whether there are technical mitigations that could be instituted to detect malicious use of the product – just to name a few.
- **Second, the where**. This is the legal piece. When examining the legal piece of a technology or product it's important to ask several questions about the country of origin. For example, to what extent do the foreign government's laws or policies permit it to compel cooperation with its intelligence activities; is there meaningful, independent judicial review; and more broadly, what are the foreign government's national security interests are as they relate to your country?
- **And third, the who**. For this, we are looking at the relationship a company may have with a foreign government. It is imperative that we examine whether a foreign government, whether

directly or indirectly, holds a financial stake in the company. It is also important to look at the extent to which a company can be influenced or susceptible to coercion.

We all know the saying, "the cybersecurity chain is only as strong as its weakest link." I believe that this framework will help ensure that our country's supply chain does not include that weak link. I welcome you to think about these three questions as you consider your role in your country's supply chain. This is an issue that we must solve together.

IV. 5G Technology

As I mentioned, one of the major supply chain risks my agency is concerned about is the rollout of Fifth Generation – or 5G – technology.

5G's impact on how it will relate to our critical infrastructure, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today as we work to secure tomorrow.

5G builds upon existing telecommunication infrastructure by improving the bandwidth, capacity, and reliability of wireless broadband services.

The evolution will take years, but the goal is to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the Internet of Things (IoT), ultra-low latency required for critical near-real time data transmission, and faster speeds to support emerging technologies.

As of June 2019, 5G networks and technologies are in development with a limited rollout in select cities around the world, including 20 in the United States.

These connections will empower a vast array of new and enhanced critical services, from autonomous vehicles, to automated manufacturing and traditional critical infrastructure, such as electricity distribution. The massive amounts of data transmitted by the Internet of Things devices on 5G networks will also advance artificial intelligence.

Given 5G's scope, the stakes for safeguarding these vital networks could not be higher.

Due to this reality, at CISA we are working with our government and industry partners to help shape the rollout of this emerging critical infrastructure, increasing its security and resilience at the design phase and reducing national security risk from an untrustworthy 5G network.

Our intent in doing so is to promote the development and deployment of a secure and resilient 5G infrastructure that enables enhanced national security, technological innovation, and economic opportunity for the United States and its allied partners.

Our work in this area will be focused on six lines of effort, which include:

- Supporting the design and deployment of 5G networks with security and resilience in mind, to include investing in Research & Development
- Promoting 5G use cases that are secure and trustworthy
- Identifying and communicating risks – including supply chain risks – to 5G infrastructure
- Promoting development and deployment of trusted 5G components
- Advancing the United States' global effort to influence direction of allied nations in 5G deployments

As new technologies, like 5G emerge, we urge all nations to conduct a careful evaluation of potential hardware and software equipment, vendors and the supply chain.

The evaluation criteria should go back to the what, the where, and the who that I mentioned earlier.

It is imperative that the international community continues to renew its efforts to incentivize security in the marketplace and ensure it is a primary consideration, alongside cost, in product development, manufacture, acquisition, and procurement.

Earlier this year, the global community made great strides at the Prague 5G Security Conference, hosted by the Czech Republic, where officials from nearly 40 countries met to discuss a set of principles on how best to design, construct, and administer secure 5G infrastructure, known as the Prague Proposal.

Establishing international cybersecurity norms, like we did in Prague, must continue with our international partners, we must continue to encourage responsible behavior and oppose those who would seek to disrupt networks and systems.

V. Information Sharing

That being said, our international cyber cooperation does not end at our risk management efforts or policy approaches.

At CISA we also work to share cyber threat information directly with our international partners.

One particular program I want you to know about is our Automated Indicator Sharing or AIS program—which is a part of CISA's effort to create an ecosystem in which, as soon as a company or federal agency observes an attempted compromise, the indicator is shared in near real-time with all our partners, enabling them to protect themselves from that specific threat before intrusion occurs.

Threat indicators are pieces of information like malicious IP addresses or the sender's address of a phishing email.

Since March 2016, we have shared more than 7 million actionable cyber threat indicators with our partners.

CISA currently has more than 250 organizations connected to our AIS server and more than 4,000 third-party AIS connections.

This commitment does not end at our borders. We also have several international CERTS hooked up to our AIS Server.

Information sharing is a crucial as we work to defend our digital networks in an increasingly hostile cyber-threat environment.

For example, in 2017 my agency received indicators from our international partners as the WannaCry ransomware spread throughout the globe, shut down everything from hospitals in the United Kingdom (U.K.) to car manufacturing in Japan. Due to the indicators shared by our international partners, we were able to get a jump- start on mitigating the threat before it spread further.

Since geographic borders of are no consequence to cyber threats, just as we saw with the WannaCry ransomware attack, it's critical that we share timely and actionable cyber threat indicators with our international partners.

If your country or organization doesn't already have a connection to CISA, I encourage you to reach out. I would be happy to connect you with the members of my team supporting our international information sharing efforts.

VI. Cybersecurity Best Practices

While information sharing is important, it is only one aspect of strengthening our collective defense. It is imperative to adopt best practices and entities to take a layered approach to security.

At CISA, we help organizations across our Nation understand their relative cybersecurity maturity by promoting best practices and by conducting risk assessments.

From a national perspective, we see some gaps between what an entity may consider adequate security for themselves or their sector and what is in the public's best interest.

For example, across the government and critical infrastructure sectors, we still see common problems such as outdated applications and operating systems. It is essential that organizations update software and operating systems with the latest patches.

The importance of strong path management was one of the main takeaways from WannaCry ransomware attack that I mentioned earlier.

The global destruction that came out of the WannaCry ransomware attack could have been significantly avoided through strong patch management practices.

My agency is using the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), along with other agency best practices, to help organizations frame what decisions should be made at what level.

I encourage you all to examine these best practices as you work to implement common cybersecurity standards within your own country.

We know that the biggest thing an organization can do to enhance their cybersecurity is to get the small things right.

Creating strong passwords, enabling multi-factor authentication, and being cautious about free Wi-Fi networks can make a huge difference in maintaining your online security.

Our networks and critical services they support are interconnected.

Implementing common security standards will go a long way in protecting our global networks.

VII. Closing

I know other countries are also looking at how to manage risks posed by technological advancement and I am eager to hear more from those represented here as to how you are approaching these issues.

The United States is tied with our Western Hemisphere partners on a wide variety of issues, from our shared values, shared security concerns, and our strong economic and cultural ties.

I am confident that by working together we can develop a common strategy to protect and defend our global cyber ecosystem.

Everyone has a role to play in the collective defense of our internet. We ask that you continue to join us, engage with us, and share with us as we collectively meet these challenges head-on.

It has been an honor to meet with all of you again. I'm now happy to take any questions you may have.

Teniente de Navío Diego Edison Cabuya Padilla Oficial Naval de Colombia de la especialidad Logístico. Ingeniero Electrónico, Profesional en Ciencias Navales, especialista en Logística, Máster en logística, Máster en Gestión de la Información y alumno del Centro de Estudios Hemisféricos de Defensa William J. Perry. Asumió la Jefatura del Departamento de Planeación del Comando Conjunto Cibernético en el 2017 y actualmente ejerce el liderazgo del Departamento de Educación, Entrenamiento y Doctrina, y del Área de Ciencia Tecnología e Innovación y de este mismo comando.

CIBERDEFENSA EN COLOMBIA:
MEJORES PRÁCTICAS Y LECCIONES APRENDIDAS

> "Con una ciberdefensa ineficaz, el DEFENSOR tiene que hacer todo perfectamente para proteger sus activos estratégicos.
> Con una ciberdefensa eficaz, el ATACANTE tiene que hacer todo perfectamente para atacarlo."
>
> Donaldson, S.; Siegel, S. Williams, C. y Aslam, A. (2015)

Comprender el Ciberespacio y su Importancia Estratégica

La globalización y el uso de las Tecnologías de la Información y las Comunicaciones, así como las tecnologías de operación en todas las áreas del conocimiento y la sociedad, trae consigo nuevos retos, escenarios y riesgos en el ecosistema digital que pueden afectar la seguridad y defensa de la nación**.** Lo anterior, aunado al contexto social que se encuentra influenciado por la cuarta revolución industrial (Figura 1), también trae cambios estructurales, volcados al entorno digital y al uso de los sistemas físicos cibernéticos, que demandan un componente fuerte de ciberseguridad y ciberdefensa por la nueva atmósfera de riesgos y amenazas, que a su vez convierte a la información en un arma estratégica, operacional y táctica poniendo a prueba la gobernabilidad de las naciones.

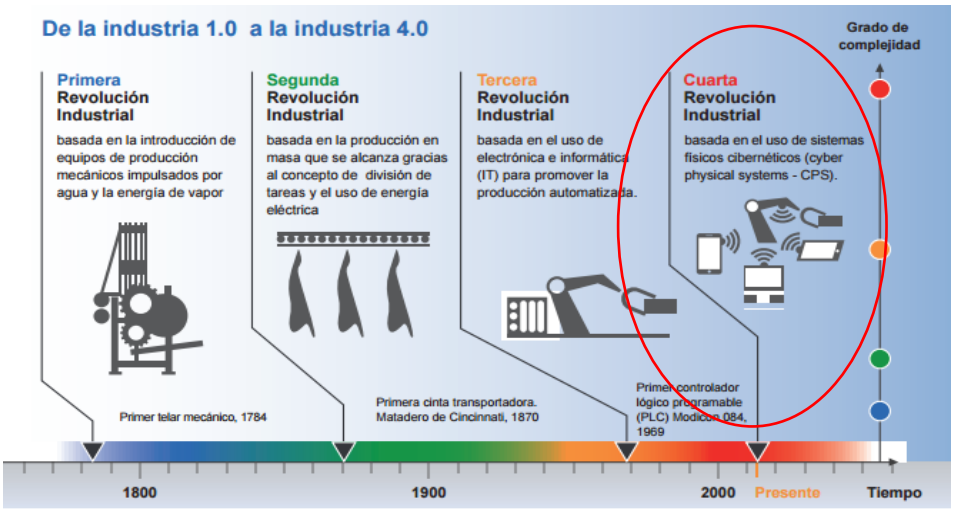


Figura 1. La cuarta revolución industrial.
Fuente: Adaptado de Engineers Journal 2016.

El ciberespacio se vuelve entonces un protagonista geopolítico siendo considerado el quinto dominio de la guerra, el cual debe ser comprendido en su complejidad. En este sentido, Colombia concibe al ciberespacio como un conjunto de capas distintas pero interrelacionadas, que permiten gestionar la complejidad del intercambio de información, así: física, lógica y ciber-persona (Figura 2).

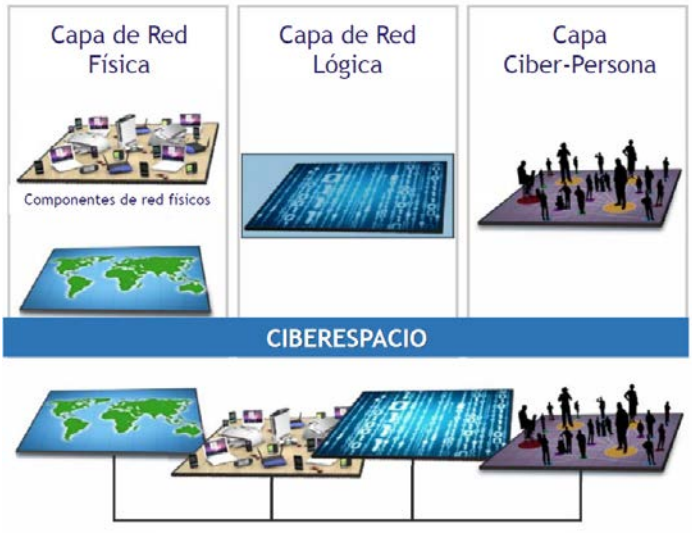


Figura 2. Capas del ciberespacio.
Fuente: Adaptado de Department of Defense – United States Goverment 2018

Más allá de sus capas, el ciberespacio tiene unas características únicas (Figura 3) que hacen que la defensa en él sea altamente compleja y un reto para las naciones.

Figura 3. Características del ciberespacio.
Fuente: Adaptado de CHOUCRI, 2012; y Cano, 2018

La complejidad del ciberespacio en su esencia se tornó en una preocupación para Colombia sustentada en el creciente riesgo que generan los ciberataques a las naciones y la necesidad de contrarrestar esta situación, como lo expone el Foro Económico Mundial en su “Reporte anual de riesgos”, donde se muestra que los ciberataques se encuentran en el cuadrante de los riesgos más probables y de mayor impacto como se puede ver en la Figura 4.

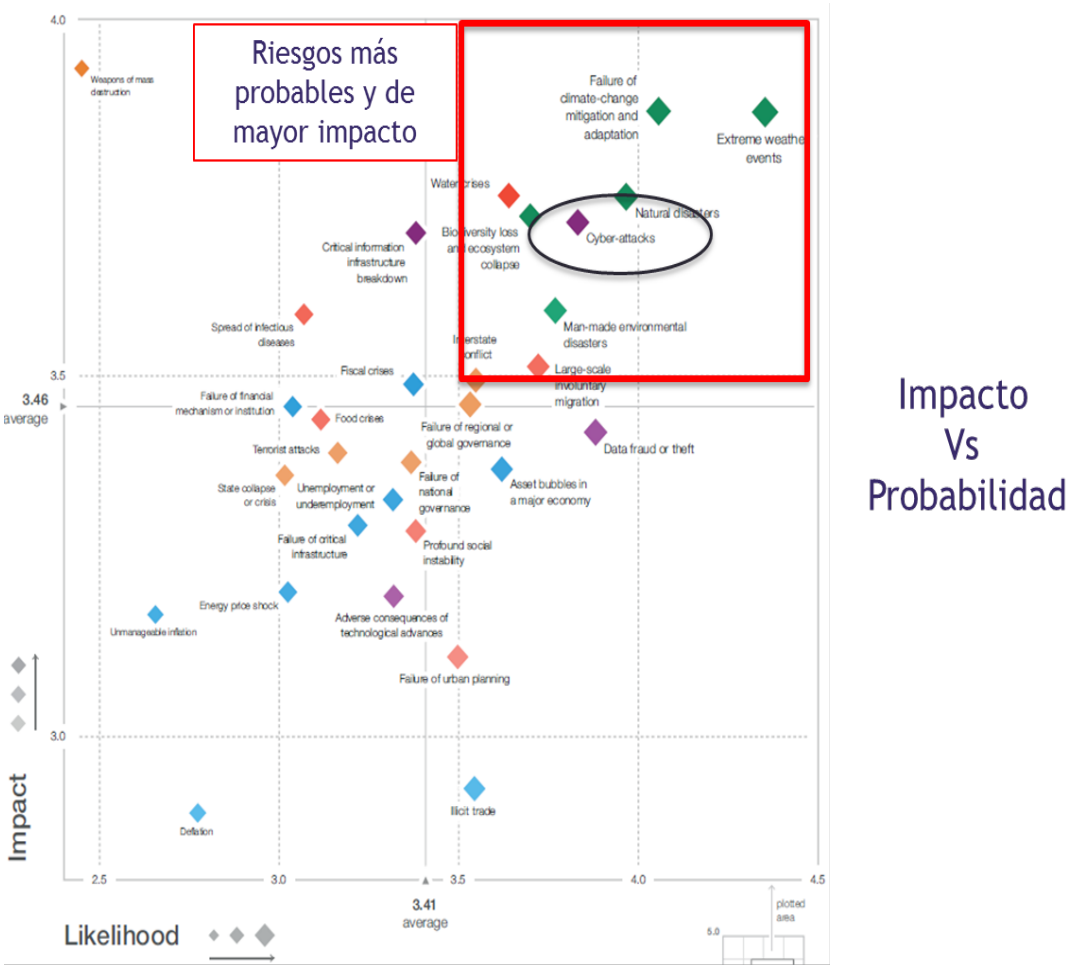


Figura 4. Panorama de riesgos mundiales.

Fuente: Adaptado de World Economic Forum 2019.

Por otra parte, estos ciberataques coexisten y se interrelacionan con otros riesgos de interés nacional, que al final generan una profunda inestabilidad social, generando efectos sobre la economía, la política, etc., que demandan un profundo conocimiento de la amenaza.

Figura 5. Línea de tiempo de riesgos más probables y de mayor impacto
Fuente: Adaptado de World Economic Forum 2019.

Comprender las Amenazas Digitales

Para afrontar los riesgos digitales se requiere comprender la amenaza, que es vista por Colombia desde dos enfoques, un enfoque técnico y un enfoque estratégico. El enfoque técnico (Figura 6) trata del conocimiento actualizado de las Tácticas, Técnicas y Procedimientos con fines ofensivos.

Figura 6. Panorama de amenazas digitales desde el punto de vista técnico
Fuente: Agencia Europea de Seguridad de las Redes y de la Información 2018

El enfoque estratégico (Figura 7) se centra en la geopolítica, considerando tres aspectos principales. Primero, las vulnerabilidades digitales (CIDOB 2018) (CIDOB 2019) relacionadas con los cambios tecnológicos que obligan a gobernar espacios que o no eran gobernados o estaban por descubrir.

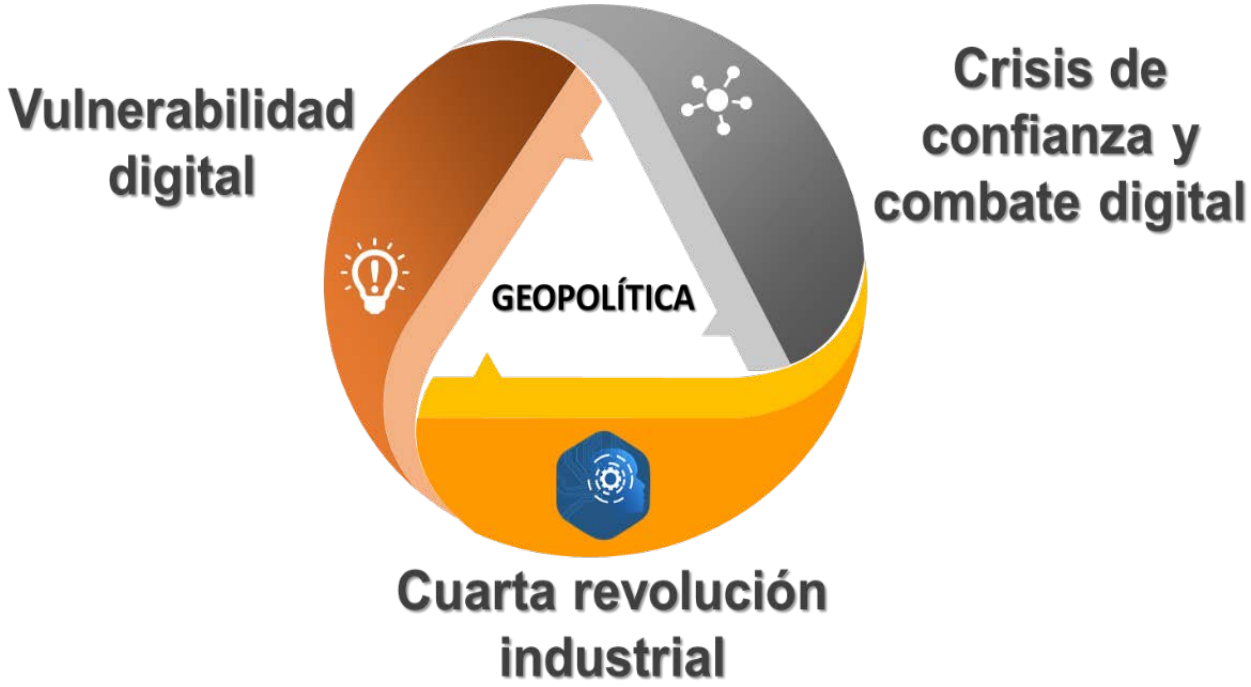


Figura 7. Panorama de amenazas digitales desde el punto de vista estratégico
Fuente: Adaptado de CIDOB, 2018 y 2019; y Cano, 2018

Segundo, la cuarta revolución industrial (CIDOB 2018 y 2019) entendida desde la perspectiva del acelerado cambio tecnológico que ya se está traduciendo en una redistribución del poder a escala global y que está alterando las bases sobre las que se fundamentan los órdenes económicos y sociales de las economías más desarrolladas; y tercero, la crisis de confianza y combate digital (CIDOB 2018 y 2019) reflejada en la transformación del uso de la (des)información en la acción política, que se traslada desde las redes sociales y las plataformas abiertas a los espacios digitales cerrados y de confianza. Esto obliga a repensar estrategias para adaptarse a los parámetros legales, tecnológicos y éticos distintos, en una sociedad fragmentada por la información.

Así las cosas, se prevé una profundización de la fragmentación y la crisis de confianza que obliga a países como Colombia a reflexionar sobre las formas de afrontar estas amenazas estratégicas que pueden transformarse en ciberataques, donde la politización y las figuras carismáticas, combinadas con mensajes positivos y nuevas representaciones - generacionales, de género, de clase e identidad- pueden ser la mejor estrategia para afrontar las amenazas (CIDOB 2018 y 2019), que pueden venir de atacantes oportunistas, *hacktivistas*, grupos criminales organizados, amenazas persistentes avanzadas o Estados (Figura 8), cada uno con sus motivaciones particulares.

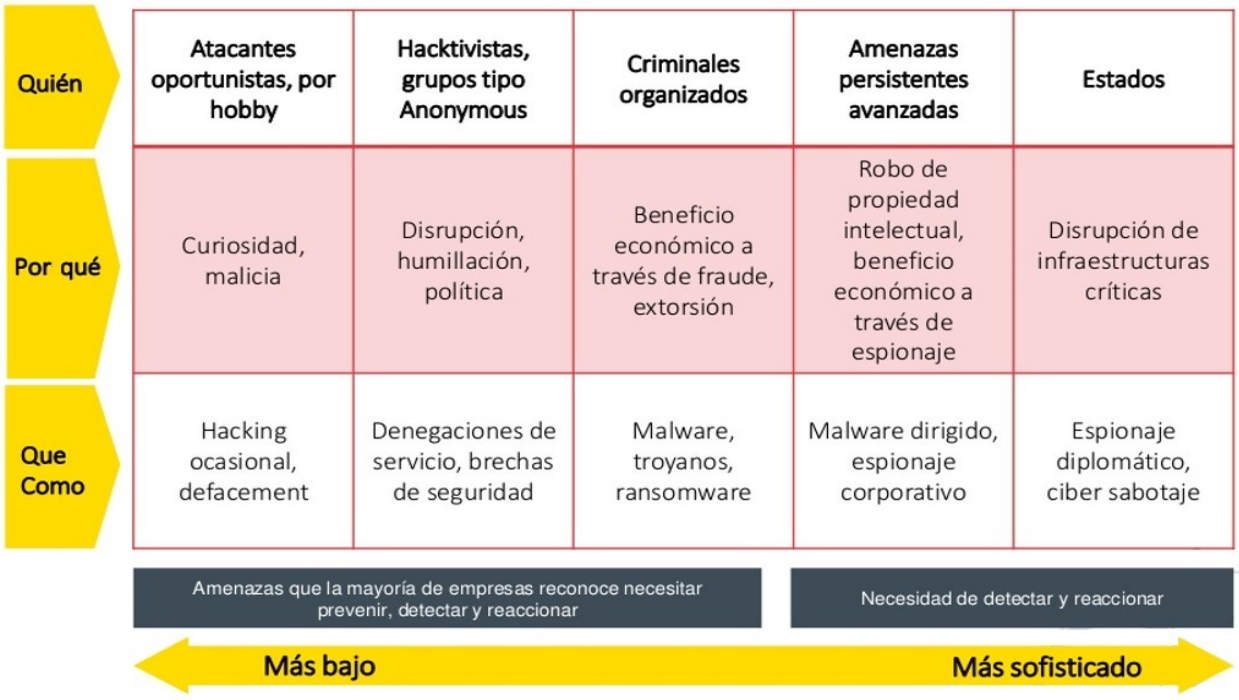


Figura 8. Panorama de actores y motivaciones de amenazas digitales

Fuente: INCIBE 2017

Esta inestabilidad social generada por el inminente riesgo de ciberataques se puede categorizar en cuatro factores de riesgo social (Cano M., 2014): conocidos, latentes, focalizados y emergentes. Estos riesgos resumen el conocimiento o desconocimiento de la nación y su entorno en temas cibernéticos y deben ser los focos de atención de las naciones para proteger sus infraestructuras críticas.

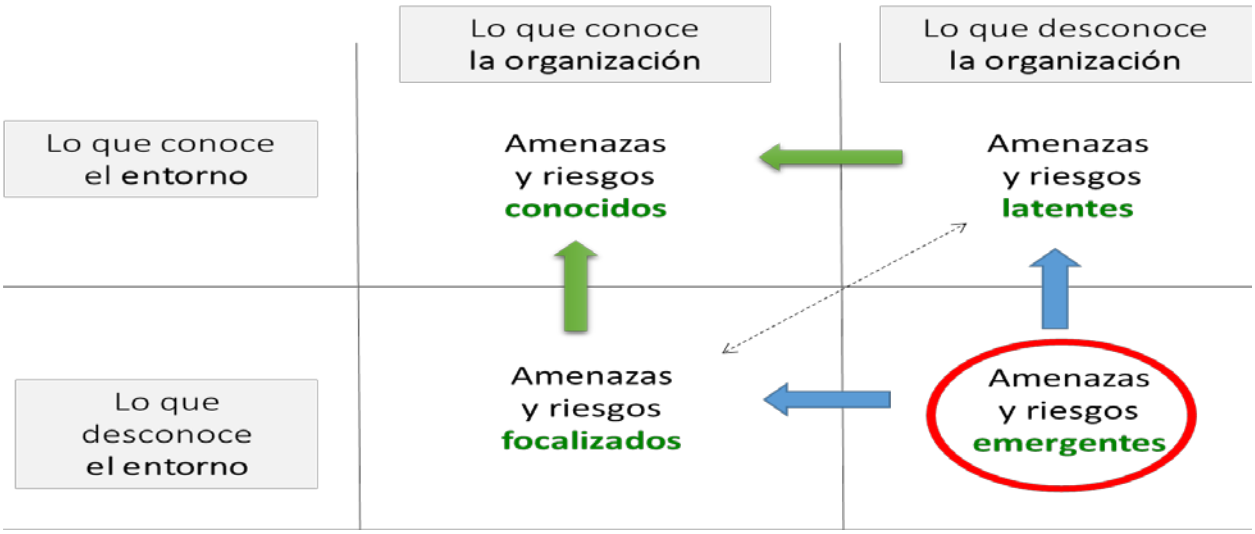


Figura 9. Ventana de AREM de los riesgos cibernéticos de la nación
Fuente: Adaptado de Cano M. 2014, y Cano 2018

Para Colombia esta categorización de factores de riesgo se puede ver acelerado por diferentes aspectos sociales, tales como (Figura 10): ciberguerra, identidad, post-verdad, hardware modificado, internet de las cosas y tratamiento de los datos.

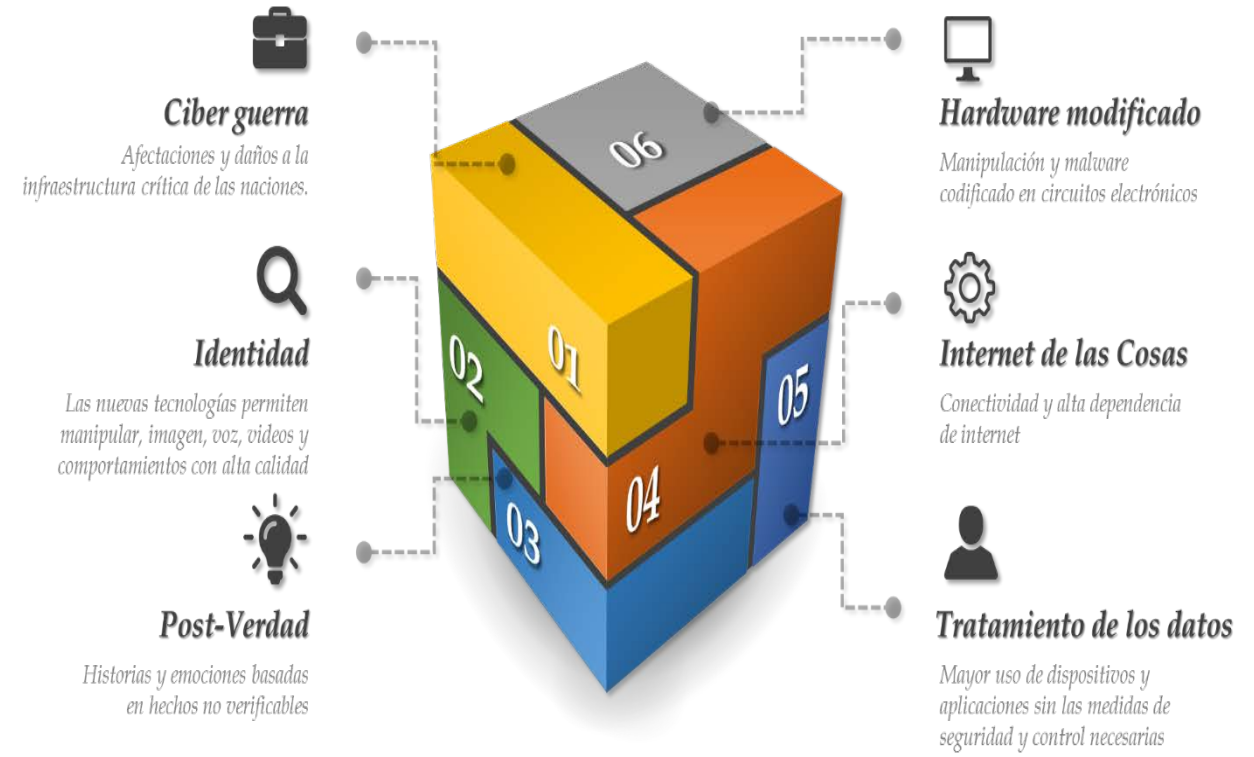


Figura 10. Aceleradores de las amenazas digitales
Fuente: Cano, 2018 y Raban, 2018

Adicionalmente a estas amenazas y riesgos identificados, se une la nueva carrera ciber-armamentista que cursan las naciones y algunas organizaciones, buscando prepararse para los presentes y futuros escenarios de guerra en el ciberespacio en ataque y defensa (Figura 11), que pueden crear efectos notorios (visibles para los usuarios y operadores de los sistemas) de (1) afectación (degradación, disrupción, denegación o destrucción) en el ciberespacio previniendo el acceso o disponibilidad total o parcial del blanco; (2) manipulación (control o alteración) de datos, redes o sistemas a través de técnicas de engaño, suplantación, clasificación, condicionamiento o codificación, orientando los efectos a repercutir en los dominios físicos (Figura 12).

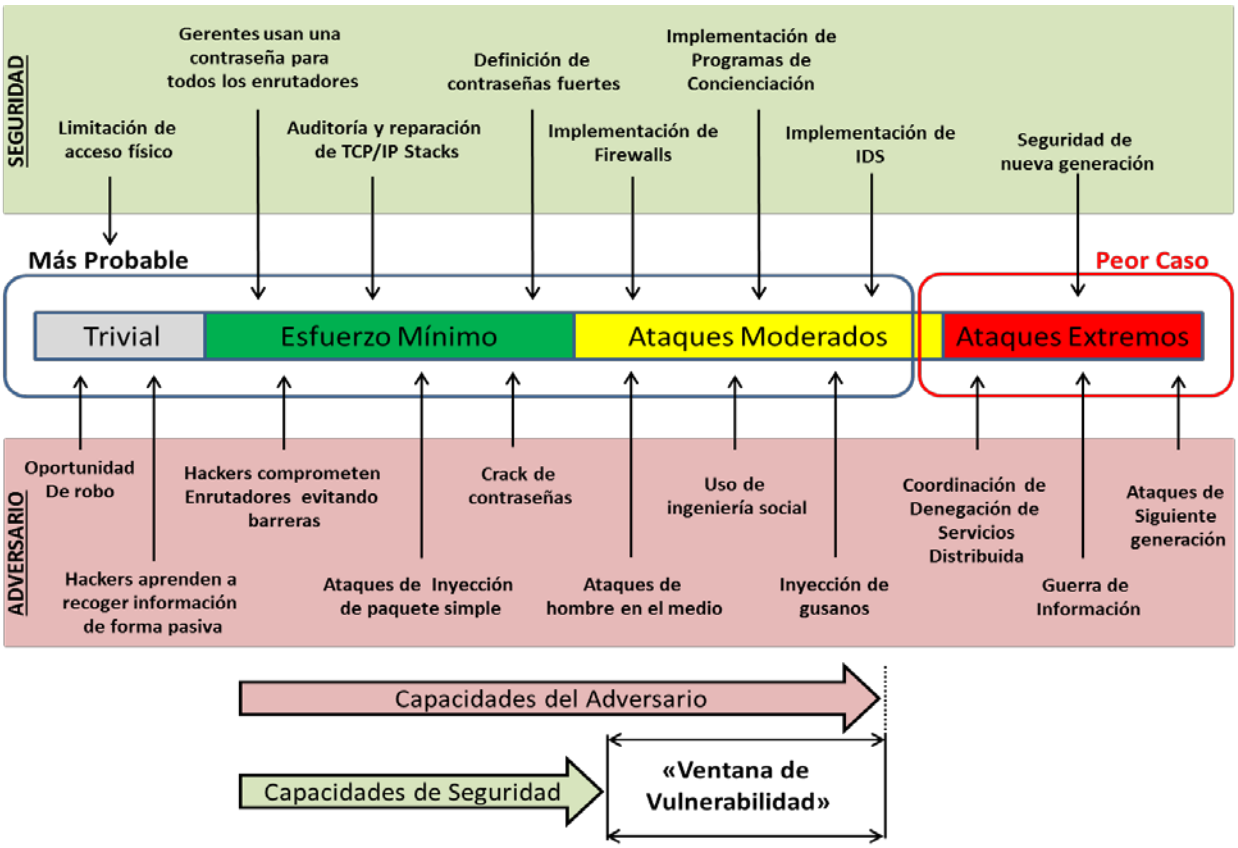


Figura 11. Carrera armamentista en ciberseguridad Fuente: Adaptado de Idaho National Laboratory, 2016

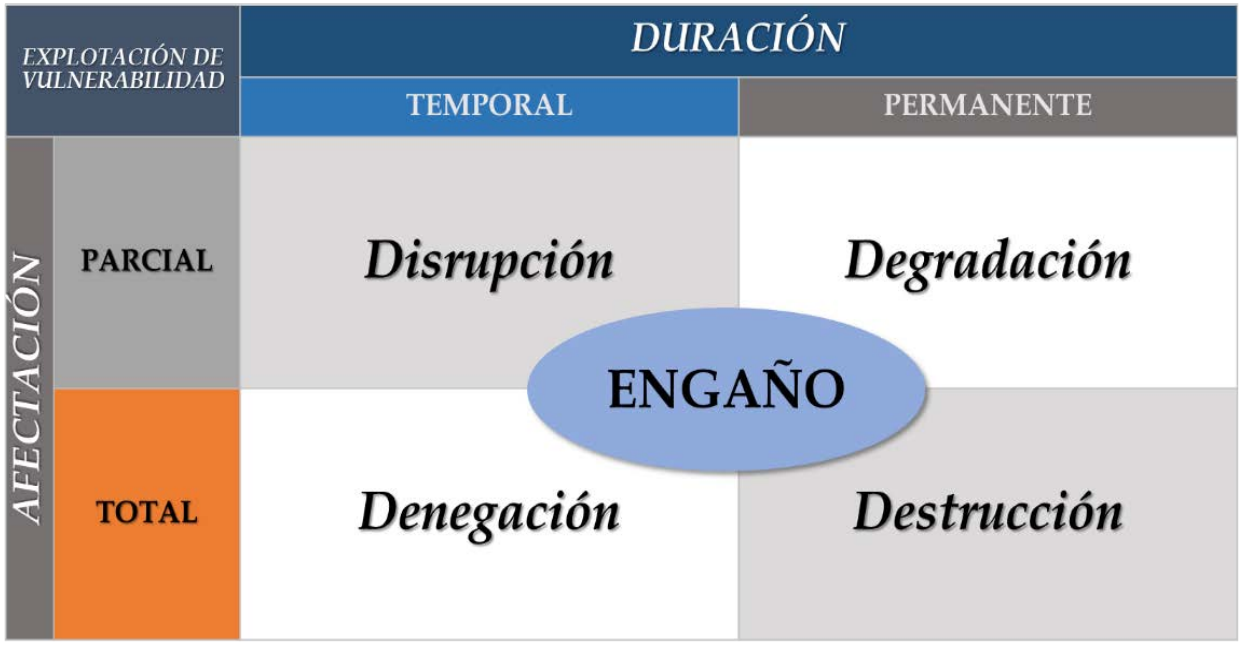


Figura 12. Carrera armamentista en ciberseguridad
Fuente: Adaptado de Schlichting, 2018; y Cano, 2018

Atender los Asuntos del Ciberespacio como Nación

Teniendo en cuenta el proceso de comprensión del ciberespacio y su importancia estratégica, Colombia desde el año 2011, ha visto la dependencia e importancia de las Tecnologías de la Información y las Comunicaciones (TIC) en los servicios esenciales de la nación y su infraestructura crítica, así como la necesidad de ser protegido de las amenazas en el ciberespacio, en aras de garantizar la sostenibilidad y prosperidad económica y social del país, por lo tanto, mediante el CONPES (Consejo Nacional de Política Económica y Social de Colombia) 3701 de 2011 (Departamento Nacional de Planeación 2011) se establecieron los "Lineamientos de Política para Ciberseguridad y Ciberdefensa", que incluyó la creación de la estructura necesaria para atender los asuntos del ciberespacio y afrontar los retos venideros. Esta estructura la conforman tres instituciones principales (Figura 13) el ColCERT (Equipo de Respuesta ante Emergencias Informáticas de Colombia), Centro Cibernético Policial y el Comando Conjunto Cibernético, este último responsable de la ciberdefensa de la nación.

Figura 13. Organización para atender los asuntos del ciberespacio.
Fuente: Comando Conjunto Cibernético de Colombia.

Así mismo, se establecieron los lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, este CONPES recogió los antecedentes nacionales e internacionales, la normatividad del país en torno al tema y los factores clave del ambiente cibernético, confirmando que el país cuenta con infraestructuras críticas cibernéticas que son requeridas para mantener la operación y gobernabilidad de la nación, las cuales se requiere identificar, catalogar, priorizar y ejercer el máximo esfuerzo para mantener una alta disponibilidad de sus servicios.

Por consiguiente, el Ministro de Defensa Nacional mediante Resolución número 7436 de 2012 de fecha 31 de octubre de 2012, aprobó la disposición No. 036 del 10 de Octubre de 2012 expedida por el Comandante General de las Fuerzas Militares, por la cual se creó y activó el Comando Conjunto Cibernético-CCOCI y se aprobó su tabla de organización y equipo TAO ‘para prevenir, detectar, neutralizar, analizar y responder ante las amenazas informáticas que atentan contra la seguridad y defensa del Estado Colombiano en el ciberespacio’. La creación de esta unidad se ha convertido en un factor estratégico que permite a las Fuerzas Militares, unificar esfuerzos para la Defensa del Estado en el nuevo dominio de guerra, “El Ciberespacio” (NATO 2016).

De igual forma, se ordenó la creación de estructuras organizacionales al interior de cada Fuerza denominadas Unidades Cibernéticas de las Fuerzas, con las cuales el CCOCI ejecutaría y coordinaría operaciones para la ciberdefensa del país de acuerdo al tipo de amenaza, rol, naturaleza, función propia a cada Fuerza y la reglamentación que se establezca.

Y es que el Ministerio de Defensa admite que la protección de la soberanía y los ciudadanos depende en gran medida de la lucha contra la delincuencia cibernética y la defensa de la Infraestructura Crítica Cibernética Nacional (ICCN). Por tanto, una de las metas de la ciberdefensa es "el desarrollo de una estrategia de cooperación conjunta, que permita generar todas las acciones necesarias para la protección de la infraestructura en el ámbito cibernético, que pueda comprometer la seguridad nacional" (Comando Conjunto Cibernético 2017, 11,12).

Posteriormente, el Plan Nacional de Desarrollo 2014-2018 (Departamento Nacional de Planeación 2014), buscó construir una Colombia en paz, equitativa y educada, mediante la estrategia para el "Fortalecimiento de los roles del Estado para el goce efectivo de derechos de todos los habitantes del territorio", la "Estrategia Nacional de Ciberseguridad" y el "Fortalecimiento de las capacidades en ciberdefensa".

En el mismo sentido el CONPES 3854 del 11 de abril de 2016 (Departamento Nacional de Planeación 2016), Política Nacional de Seguridad Digital, estableció la consolidación y fortalecimiento del Comando Conjunto Cibernético (CCOC) como ente rector en ciberdefensa para el país, y la creación de un Centro Cibernético Conjunto (Comando Conjunto Cibernético 2017, 11,12), además de incluir la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Basado en cuatro principios fundamentales y cinco dimensiones estratégicas que permiten el fortalecimiento de las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

Por último, durante el año 2018 el Comando General de las Fuerzas Militares de Colombia llevó a cabo el proceso de reestructuración de su organización, que buscó transformar al Comando General en una organización relevante para la toma de decisiones del Ministerio de Defensa Nacional, del Presidente y primordial para la conducción de campañas militares. Donde se evidenció la necesidad de revisar la doctrina y procedimientos para ejercer la ciberdefensa en las Fuerzas Militares de Colombia.

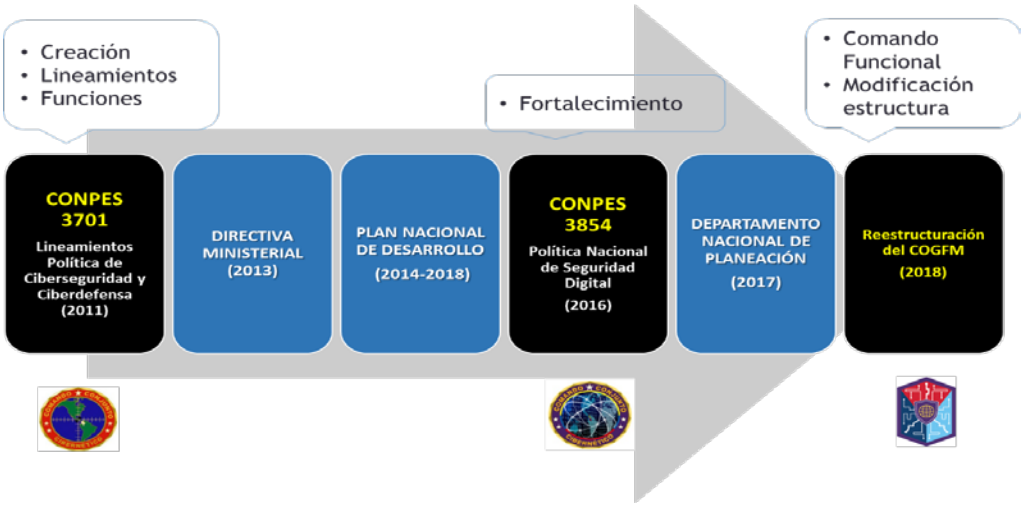


Figura 14. Proceso de conformación del Comando Conjunto Cibernético
Fuente: Comando Conjunto Cibernético de Colombia.

Como resultado del proceso anteriormente relacionado, el Comando Conjunto Cibernético (CCOCIC) tiene como misión operacional "Ejercer la ciberdefensa y conducir operaciones militares cibernéticas a nivel estratégico, para la seguridad y defensa de la Nación en el ciberespacio", adicionalmente tiene una misión de carácter estratégico que es "Ejercer la gobernanza de las Infraestructuras Críticas Cibernéticas Nacionales". En este sentido la Figura 15 resume las áreas de responsabilidad del CCOCI, teniendo en cuenta la porción del ciberespacio en el que se requiere actuar y la responsabilidad sobre este.

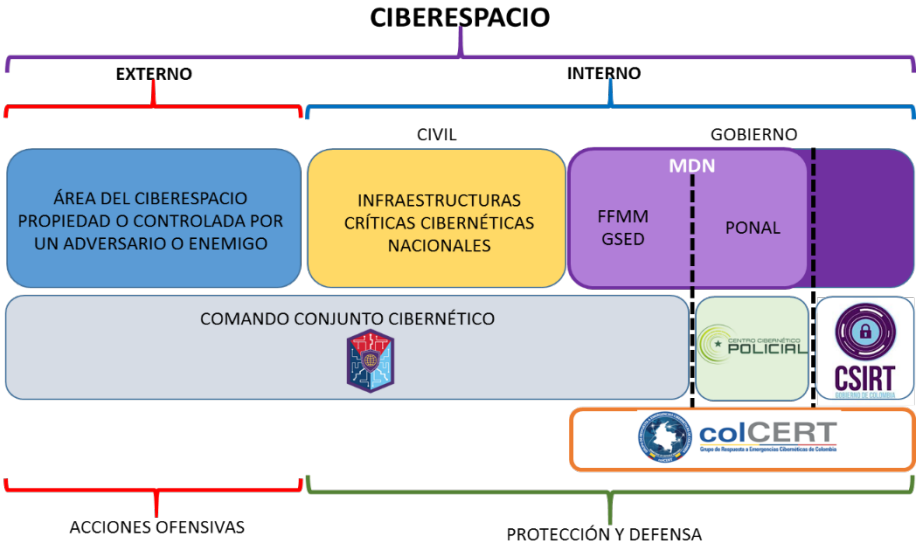


Figura 15. Áreas de responsabilidad del Comando Conjunto Cibernético
Fuente: Comando Conjunto Cibernético de Colombia.

Planeación por Capacidades

Para afrontar las responsabilidades en el ciberespacio asignadas por el gobierno al Comando Conjunto Cibernético, se creó el "Sistema Integral de Ciberdefensa" en las Fuerzas Militares, que refleja las capacidades cibernéticas para el cumplimiento de la misión institucional y está compuesto por los subsistemas de inteligencia cibernética, defensa cibernética, ataque cibernético, ciberseguridad estratégica, excelencia cibernética y observatorio cibernético fundamentado en el subsistema de soporte cibernético, los cuales se emplearán en tiempos de paz y guerra para el ejercicio de la ciberdefensa y la conducción de operaciones cibernéticas estratégicas, operacionales o tácticas en forma conjunta, coordinada, combinada y multinacional para disuadir de manera creíble posibles adversarios internos o externos o para ejercer la respuesta oportuna, legitima y proporcional ante amenazas o agresiones de naturaleza cibernética que puedan afectar la seguridad y defensa nacional.

Este sistema planteado se alinea a la metodología adoptada por el Ministerio de Defensa Nacional de Planeación por Capacidades, que busca establecer una taxonomía de capacidades para el sector defensa y sobre ella determinar las brechas de capacidad, priorizaciones y necesidades para el cumplimiento de la misión institucional. En este sentido, el Sistema de Capacidades de Ciberdefensa contempla una línea base para el ejercicio de la ciberdefensa que es el "Soporte Cibernético" y dos subsistemas de capacidades que son: los "Subsistemas Operacionales" que tratan de las capacidades necesarias de carácter operativo y táctico para ejercer la ciberdefensa de la nación; y los "Subsistemas de Sostenibilidad" que buscan mantener y fortalecer las capacidades operacionales en el tiempo (Figura 16).

Figura 16. Sistema Integral de Ciberdefensa de Colombia
Fuente: Elaboración propia.

Cyber Soft Power

De las capacidades anteriormente mostradas se resalta para Colombia la "Ciberseguridad Estratégica" como la capacidad de gobernanza cibernética de las Infraestructuras Críticas Cibernéticas Nacionales (ICCN), donde se aplica el "Cyber Soft Power" o la capacidad de obtener un estado deseado en el ciberespacio a través de la atracción y persuasión. En este sentido, y debido a la carencia de normatividad que obligue a las Infraestructuras Críticas Cibernéticas se recurrió al empleo del Cyber Soft Power para liderar las iniciativas de protección y defensa cibernética de las ICCN, así como para crear conciencia en los lideres sectoriales de Colombia.

Para lograr este objetivo se adelantó un proceso de dos fases, una del 2013 al 2015 y otra del 2016 a la fecha. La primera fase buscó crear una estructura organizacional para reunir a los principales representantes de infraestructuras criticas cibernéticas, para ello se nombró unos lideres sectoriales provisionales para crear un equipo de trabajo que definiera la metodología a usar para desarrollar una acción sostenida en el tiempo que permitiera conseguir los objetivos planteados, así como metodologías para la identificación y priorización de infraestructuras críticas cibernéticas (Figura 17)

Figura 17. Fase I Infraestructuras Críticas Cibernéticas Nacionales
Fuente: Comando Conjunto Cibernético

Posteriormente en la segunda fase, se identificaron los sectores estratégicos desde la óptica cibernética, donde se establecieron 13 sectores estratégicos y sus respectivos líderes sectoriales con los que se llevarían a cabo las iniciativas del ámbito cibernético a nivel nacional, y para este fin se establecieron las reuniones mensuales de ICCN con el propósito de crear conciencia situacional, generar cooperación cibernética y establecer mesas de trabajo para generar productos de impacto a nivel nacional, entre los cuales se elaboraron: catálogo anual de ICCN, Plan Nacional de Protección y Defensa de ICCN y Planes Sectoriales de Protección y Defensa. A la fecha se continúa trabajando en la creación de normatividad y procedimientos asociados a la protección y defensa cibernética tales como planes de operador, tácticas, técnicas y procedimientos de defensa, etc.

Figura 18. Fase II Infraestructuras Críticas Cibernéticas Nacionales
Fuente: Comando Conjunto Cibernético

Este proceso descrito le permitió a Colombia generar una sinergia nacional alrededor de los asuntos del ciberespacio, con resultados muy satisfactorios y con una buena proyección de crecimiento y de generación de contenidos y normatividad de interés para la protección y defensa de las ICCN.

Como conclusión y teniendo en cuenta el caso de estudio de Colombia, los países deben entender el panorama internacional y nacional de amenazas digitales para conformar un sistema de capacidades suficiente y flexible para afrontar estas amenazas, con una estructura de cooperación con las Infraestructuras Críticas Cibernéticas que permitan hacer una gobernanza cibernética efectiva y coercitiva con fines de impacto nacional.

Bibliografía

1. **Engineers Journal.** 2016. "Future trends in engineering: global urbanisation and the fourth industrial revolution." Junio 14. Accessed Febrero 10, 2018. http://www.engineersjournal.ie/2016/06/14/future-trends-in-engineering-global-urbanisation-the-fourth-industrial-revolution.

2. **Department of Defense - United States Goverment.** 2018. *Joint Publication 3-12 Cyberspace Operations.* United States: Joint Force Development.

3. **CHOUCRI, N.** 2012. "Cyberpolitics in international relations." MIT Press.

4. **Cano, Jeimy**. 2018. "Memorias Congreso Internacional Ciberseguridad Escuela Superio de Guerra." Bogotá.

5. **World Economic Forum.** 2019. "weforum." *The Global Risk Report 2019.* Accessed 2019. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf.

6. **Agencia Europea de Seguridad de las Redes y de la Información.** 2018. "Cyber Threat Landscape." ENISA. Accessed Octubre 24, 2019. https://etl.enisa.europa.eu/#/.

7. **CIDOB.** 2018. *El mundo en 2018: diez temas que marcarán la agenda internacional.* Accessed Octubre 22, 2019. https://www.cidob.org/es/publicaciones/serie_de_publicacion/notes_internacionals/n1_186/el_mundo_en_2018_diez_temas_que_marcaran_la_agenda_internacional.

8. —. 2019. *El mundo en 2019: diez temas que marcarán la agenda internacional.* . Accessed Octubre 23, 2019.

https://www.cidob.org/publicaciones/serie_de_publicacion/notes_internacionals/n1_208/el_mundo_en_2019_diez_temas_que_marcaran_la_agenda_global.

9. **INCIBE.** 2017. "Memorias Cybersecurity Summer Bootcamp." *Motivaciones de las amenazas cibernéticas.* Leon (España).

10. **Cano M., Jeimy J.** 2014. "criptored." *Ventana de AREM.* Accessed Febrero 12, 2018. http://www.criptored.upm.es/descarga/Ciberdefensa-14w.pdf.

11. **Raban, Y. & Hauptman,** A. 2018. "Foresight of cyber security threat drivers and affecting technologies."

12. **Idaho National Laboratory**. 2016. "The Electronic Arm Race of Cybersecurity." Accessed Febrero 12, 2018. https://abm-website-assets.s3.amazonaws.com/impomag.com/s3fs-public/legacyimages/0703/Fig1a.gif.

13. **Schlichting, A.** 2018. "Assessment of Operational Energy System Cybersecurity Vulnerabilities." MITRE Corporation. https://www.mitre.org/publications/technical-papers/assessment-of-operational-energy-system-cybersecurity-vulnerabilities .

14. **Departamento Nacional de Planeación.** 2011. *CONPES 3701 - Lineamientos de Política Para Ciberseguridad y Ciberdefensa.* Bogotá.

15. **NATO. 2016**. "NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit." Warsaw Summit. Julio 21. Accessed Julio 3, 2018. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html.

16. **Comando Conjunto Cibernético. 2017.** *Plan Nacional de Protección y Defensa para la Infraestructura Crítica Cibernética de Colombia.* Bogotá: Comando General de las Fuerzas Militares de Colombia.

17. **Departamento Nacional de Planeación . 2014.** *Plan Nacional de Desarrollo 2014-2018* . Bogotá. Departamento Nacional de Planeación. 2016. *CONPES 3854 - Política Nacional de Seguridad Digital.* Bogotá.

Dr. Marty Trevino Jr is a Data & Decision Scientist focused on improving strategic decision making through Visual Analytics, Cognitive and Behavioral Psychology and the Neuroscience of decision making. He is the Director of Security Strategy and Analytics at a leading Silicon Valley cybersecurity firm, the senior technical advisor to the Inter American Defense Board and visiting professor at the National Defense University. Previously, he served at the National Security Agency (NSA) of the USA

HIGH-ORDER AUGMENTED INTELLIGENCE
AUGMENTED COGNIZANCE AND NEXT GENERATION ADVANCED ANALYTICS
THE ART-OF-THE-POSSIBLE

"The single most important element of organizational success is Strategic Decision making." – the Author

"In specific analytical tasks, computer beats the human an overwhelming percentage of the time. But when computers and humans are paired together and pitted against a computer the human/computer pairing wins every time". - the Author

Introduction

As the 21st Century matures Strategic Decision Making (SDM) remains a central element to organizational success. This tenet stands true regardless of organizational type (commercial industry, government or military) or location. This statement is supported by innumerable and well-documented failures to recognize shifts in the operational landscapes of the respective organizations, be them military, intelligence or commercial for profit. The need for tools and methods to improve strategic decision making within OODA loops is beyond debate.

The principal challenges to improving strategic decision making as seen at one level of analysis is two-fold. First ever-increasing amounts of data and information available to decision-

makers and a resulting cognitive overload from this phenomenon. Second, the innate structure of the human brain coupled with the cognitive error pathways all humans are 'wired' to make. The central question for technical experts and decision scientists is how to capture and transform data and related contextual information into a cogent delivery able to overcome both the design of the human brain and its related cognitive error tendencies. If done effectively this will have a two-fold effect; first, to reduce cognitive overload and second, to improve the quality and speed of strategic (creative) decision making. Until now, this has been a wicked problem;[1] but a unique convergence of technology, machine learning, and scientific knowledge is on the verge of producing an elegant technical solution.

Conceptualizing Next Generation Decision Making

The ability to radically alter strategic decision making promises to permanently alter the military, intelligence, and commercial for-profit eco-systems. Improved strategic decision making and faster OODA Loops through the use of technology represents one of the greatest opportunities to create unique strategic advantages of the digital age.

The military and intelligence services of virtually every nation have historically expended significant resources to capture and harvest data to inform decision-making and attain desirable outcomes. Yet despite those investments, long-established cognitive and organizational impediments consistently undermine efforts 'data-driven' decision making.

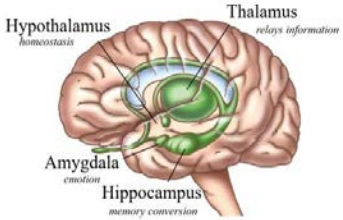
At the mid-level, military and intelligence officers and their commercial for-profit counterparts routinely embrace data to inform tactical decisions. These decisions are often prescriptive vs. creative in nature, I.E. scheduling, ordering, production rates, process controls, etc. Prescriptive decisions are less prone to cognitive error than creative decisions. This is partially due to the decision-maker having less latitude in the decision process as well as more readily acceptable information E.G. a widget consumption history from which to base their current order. Strategic or creative decisions are far more to prone cognitive error attributed to the structure of

[1] A wicked problem is a problem that is difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognize. It refers to an idea or problem that can not be fixed, where there is no single solution to the problem.

the brain as well as errors that fall into the behavioral psychology area. These include heuristic errors, bias, Big 5 trait skewness, trivialize and or facing personal risk.

Researchers and authors have addressed the functioning of decision processes in the human brain in a wide variety of situations. These authors include less technical works such as Malcolm Gladwell's *Blink* which addresses "Thin Slicing". The foundation for Gladwell's work can be directly traced back to the groundbreaking research by Nobel Prize Laureate Daniel Kahneman and his long-time partner Amos Tversky. Kahneman's 2011 book, *Thinking, Fast and Slow* is widely regarded as a seminal work and required reading of anyone desiring to understand human decision processes. Iain McGilchrist's work *The Master and his Emissary* provides a technical 'deep dive' into the hemispheric functions of the brain. Numerous other detailed works are available to include detailed overviews of the neurological constructs of the brain vs. the outcomes of the interactive processes. Two recommended but deeply technical literary works are *Neuroscience of Decision Making* edited by Vartanian and Mandel and *The Neuroscience of Risky Decision Making* edited by Reyna and Zayas.

The dilemma of improving creative decision making as it relates to data and analytics is a multi-dimensional challenge. First, the volume of information[2] available to decision-makers is unabated and increasing at an increasing rate. The result of available massive amounts of data is often cognitive overload. Cognitive overload reinforces the brain's inherently lazy approach to updating its internal model of the world by simply ignoring most of the information available to it. We are made to believe we see everything, but we are mostly on autopilot; It is the human brain's greatest illusion to "fool" us into thinking we are aware of everything when we are in reality, aware of so little. Second, is the structure of the brain and how its organs and systems work together and against each other during the decision making process. At one level of analysis, you can divide the human brain into major sections with the Limbic system being paramount. This system is composed of several organs each with specific functions related to decision making and can aptly be called the center of decision making for the human brain. The Limbic system formulates emotions such as trust and loyalty all



[2] Limiting the term "information" to encompass data and analytics but not textual, audio or other general information.

the while having no capacity for language. This is the region of the brain where “gut” feeling comes from, and is at the center of our disregarding of data because “it just doesn’t feel right”.

Third is the formulation of our internal model of the world. Enabling us to navigate the world is an “internal model’ which is developed in the Thalmus. Our model of the world enables us to function in a constantly changing and immensely complex world. This model is constantly being updated by our senses as they search for anomalies to the believed reality. One issue with the formulation of the internal model where data or analytics is concerned is that these are normally interacted with through the Cortex. Information is transmitted from the Cortex (the eyes) to the Thalamus (where the Internal Model is formulated) and back to the Visual Cortex (perceptions of reality stored in the back of the brain). The issue lies in the volumes of information being sent to the Thalamus. The Visual Cortex sends approximately 6 times more information to the Thalamus as it updates our internal model of the world than does the Cortex. In short, our model of the world is built on six times more information from what we already believe to be true than what we are seeing with our eyes. Examples of how this intractable equation wreaks havoc on decision making are innumerable and found in every domain of creative decision making. This is how American military forces were caught off guard by the German assault at the battle of the bulge and the Chinese assault in Korea. In both instances, ample intelligence of the enemy’s intent and presence was available and simply ignored because the respective commanders didn’t believe the intelligence as it conflicted with their internal model. The fourth and final consideration to improving decision making is to be found in the Cognitive abilities and Behavioral (Psychology) traits of the decision-maker. More attention is given to the latter as the Big 5 behavioral traits can be assessed at speed and scale algorithmically by examining textual messages - emails, texts, and pictures posted on social media. Other relevant psychological attachments such as Cohesion and Organizational Commitment (OC) can also be assessed algorithmically. These constructs are important to decision making as every individual weighs the personal consequences of making risky decisions. A person with a high level of Cohesion and Organizational Commitment making a high-risk decision with personal consequences is likely to make a very different decision than a person with low levels of Cohesion and OC.

Thus, the augmented cognizance of next-generation decision AI will constitute a form of High Order Augmented Intelligence (HOAI). This technological construct will be formulated

around an Artificial Intelligence that is centric to the decision-maker, understanding their cognitive abilities and heuristic pitfalls, behavioral traits, stress level, the neuroscience of decision making. This system will be cloud-based, utilize High-Performance Computing power when necessary and interact with its human partner through all forms of computer-human interaction to include voice and natural language processing. Once Quantum computing becomes a reality and associated new machine learning techniques are developed, HOAI will be quantum enabled and evolve into a true decision Artificial Intelligence.

High Order Augmented Intelligence – How

It is the belief of this Scientist and other practitioners that a unique convergence of Technology, Tradecraft, and Understanding is occurring and this convergence has the potential to radically augment strategic decision making. The technology is comprised of Cyber-Physical Systems (CPS) – specifically sensors able to detect behavioral patterns (eye movement, data/information selection, time spent on information, stress levels, etc.), underpinned by Machine Learning (ML) designed to identify behavioral and decision patterns at the individual level within domains of expertise. ML would also provide understanding and knowledge contained in numerous scientific disciplines related to decision making – I.E. risky decision making, economic gain and loss theory, cognitive and behavioral psychology and others. To dramatically oversimplify, we can now detect physiological and psychological manifestations of the influencers and inhibitors of creative decision processes in real-time – at speed and scale. Sensors can detect eye movement over data, the amount of time spent on data., identify elevated job pressure on the individual, any Big 5 trait, even relevant psychological constructs such as organizational commitment.[3] All the required information to make these assessments can be gathered and computed via individually centric sensors, open-source data (click preferences, social media posts, sentiment of texts, posted pictures.) and assessments and correlations made via machine learning. We stand at the cusp of a new era of High Order Augmented Intelligence designed to act as an individually tailored Sixth Sense to decision-makers.

[3] Both neuroticism and organizational commitment are peer reviewed psychological constructs with valid measurement instruments

The Failure of Purist Approaches

Strategic Decisions are fundamentally creative processes in the human brain. The evidence for this understanding is derived from Cognitive and Behavioral Psychology, Decision Neuroscience, as well as a plethora of anecdotal evidence gathered over the centuries. We see the manifestations of this truism in the failure of those advocating "data-driven" and "evidence-based" and other similarly conceived decision-making frameworks. Practitioners of Accounting, Finance, Business Intelligence, Data Science and others have been rebuffed time and time again by senior officers with statements like, "I don't care what the data says" or "I simply don't trust the numbers". One well-known expert working for a data visualization company, openly stated at a Gartner conference in 2015 that "people don't make decisions based on data – they make decisions based on what their gut tells them". This painfully true statement bluntly confirms what countless proponents of data and evidence-based decision making know all too well – that their efforts are rarely influential at the strategic level of decision making.

In attempting to influence what is a mind-bogglingly complex interaction of these major decision systems within the human brain, Data Scientists, Business Intelligence specialists, and User Interface (UI) designers have approached the problem from a data or resonation lens. An overwhelming amount of time is spent on the accuracy, precision or other aspect of the data. In the rare case that data-centered approaches were multidimensional, they were woefully, overly simplistic. This is exemplified by commonly accepted and advanced notions – "all data must tell a story", "use lots of Pie charts and dials", select "positive colors", "no more than 3 pieces of information in a single view" etc. This is not to say that all these notions were wholly inaccurate, rather that they simply do not influence decision making in the way hoped for – and never will. It is widely understood that a coherent data-informed "story" often resonates more deeply than an amalgamation of data or visual analytics. This is due to the complex way that human memory functions and millions of years of learning through precisely such means. However, to state that any of the notions alters the formulation of one's internal model and improves creative decision processes is nothing short of stupid.

This scientist will emphatically say that all the positive color selection, storytelling, and increased system functionality, in the absence of a deep understanding of decision neuroscience, cognitive and behavioral psychology, of decision making, will not overcome often a highly disagreeable senior decision-makers' innate trust of their acutely developed System 1 decision-making process.[4][5] Data-driven decision making is as dead as Latin, its advocates' naive fools and decision-makers are worse off suffering from an ever-increasing level of cognitive overload.

Every Decision Maker is Different

The statement that every decision-maker is different is rarely contested by Data Scientists and User Interface developers, yet how decision-makers are different is rarely discussed at a meaningful level of analysis. One such level is how different decision-makers will scan a computer interface and the analytics it contains in search of awareness and understanding. In short, every decision-maker will scan an interface differently based on their cognitive abilities, behavioral traits, environmental factors (pressure on them, level of organizational risk, personal danger, etc.) and their preconceived notions of what they want to get out of any scan of data. And while intuitive once stated, very few UI designers take these factors into account when attempting to construct features that will improve decision making. In fact, most UI design efforts to address this problem have been limited to the ability to select graph types on 'out of the box' interfaces of business intelligence systems. Understanding the Intractable Equation of information flow from the Cortex and Visual Cortex to the thalamus (6 to 1) painfully illustrates that any focus on enabling the user to select a more attractive graph type or flowery color in the hope of improving a creative decision process is a nearly idiotic endeavor.

Research into how individuals 'scan' a User Interface has advanced considerably over this decade but can be directly traced to the Psychologist Paul Yardis who in the 1960's conducted a series of experiments to determine how much of what our eyes saw 'registered' in our brain. Yardis was able to track the eye movements of test subjects examining a painting known as *The Unexpected Visitor*.

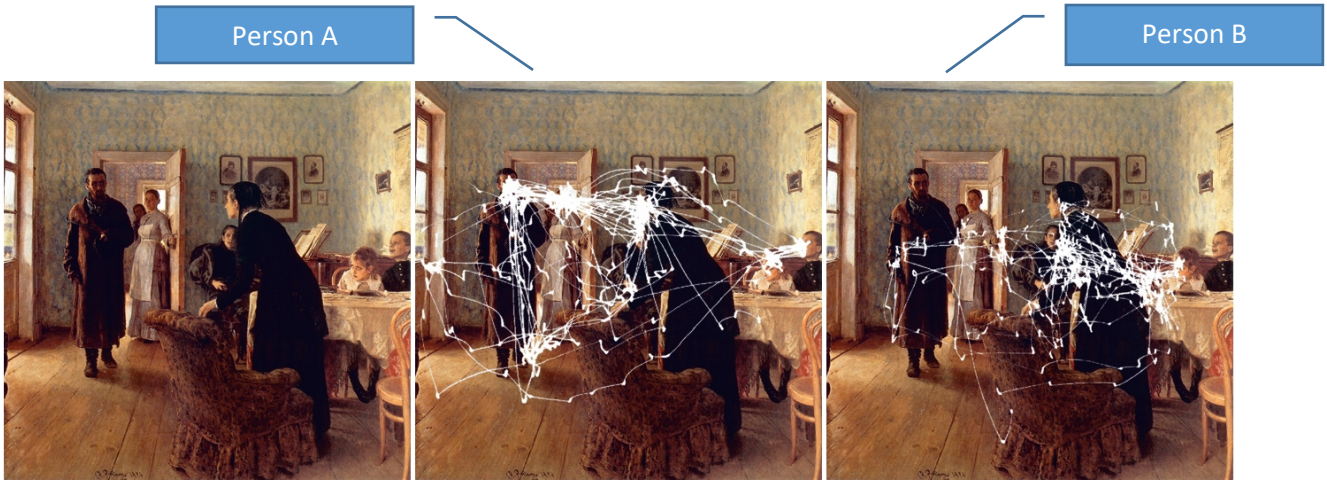
[4] System 1 is a reference to Daniel Kahneman, seminal work and duel system theory
[5] Disagreeableness is a Psychological Big 5 personality trait. It is visible and measurable

Yardis then asked the test subjects a series of questions as to the details of what they remembered about the painting. What Yardis found was revolutionary at the time. This was that individuals universally believed they had a good understanding of the details of the painting. Yet, when asked specific details virtually everyone failed to recall specific and obvious details. This was validation that the mind fools us into believing we see everything when in fact we do not – even when attempting to do so. The second stunning discovery made by Yardis was that every person examined the painting differently based on what they expected to find. In short, their prior life experience and preconceived notions have a greater impact on their perception of the painting than did their direct observation. This was a stunning validation of the Intractable Equation at work.

Today eye-tracking devices make this type of assessment easy and lend insights into how structurally a UI should be configured to an individual decision-maker. HOAI will also utilize eye tracking in association with other sensors on the body to identify flaws in data analysis and degrees of resonance of certain analytics and then make changes and give verbal guidance to correct heuristic errors such as spending too little time on a particular set of analytics.

In the picture below eye movement is clustered to illustrate how a test subject interrogated the painting. This lends incredible insight into what this test subject consciously and unconsciously viewed as important.

In the picture below the differences between how person A differed in their interrogation of the same painting from person B.



Flawed Decision Making – A Deeper Understanding

Daniel Kahneman's work "Thinking, Fast and Slow," arguably represents the best place to begin to understand the necessity for High Dimensional Augmented Intelligence. Kahneman proposes that all human decision-making is governed by two separate but codependent systems: "System 1," which is fast, instinctive and emotional, and "System 2," which is slower, more deliberative, and more logical. The human brain relies on System 1 to recognize people, objects, situations and respond quickly to each. Experience developed over time allows us to rapidly recognize the information before us and respond in an instant, or "without even thinking," as we tell ourselves. Thus, a problem that might vex us early in our career can be answered instantaneously later, the result of practice and experience. When confronted with something new or unusual, however, we must rely on System 2, which applies

reason and logic to interpret the input. Unfortunately, as Kahneman points out, this takes effort and human beings are instinctively intellectually lazy.

"When faced with a difficult question," Kahneman writes, "we often answer an easier one instead, usually without noticing the substitution." Kahneman calls this "intuitive heuristics." Worse, he describes humans' "excessive confidence in what we believe we know and our apparent inability to acknowledge the full extent of our ignorance and the uncertainty of the world we live in." For executives, this manifests itself in what Kahneman calls the WISIATTI fallacy, or "What I see Is All That There Is." This, in no uncertain terms, is a heuristic error in judgment hs been seen with great frequency in senior-level decision-makers.

These two factors contribute greatly to our struggle to think analytically and to use data and advanced analytics to guide us to better decisions. Yet we would be mistaken to completely discount the logic and analysis that takes place in an instant when executives apply System 1 thinking to complex problems. Valid intuitions absolutely do develop over time, as we learn to recognize elements or patterns and learn to apply that knowledge to novel situations. Experience, intuition, understanding, and knowledge do make an expert.

The trouble is, System 1 decisions are like a black hole to us – they happen so rapidly that, to an outsider, they appear to be made without any consideration of facts. For Quants or data people, it's as if senior leaders are ignoring the data at their fingertips. Yet to the infinite frustration of the Quants, executives rarely can explain their reasoning, falling back instead on fuzzy statements like, "my gut tells me" or "it just feels like" or even "I don't believe."

Executives are certainly capable of both System 1 and System 2 decision-making but the human brain is predisposed to simplify questions so that they can be addressed automatically by System 1. In so doing, the brain often introduces errors by changing the way a question is framed or by misapplying erroneous or irrelevant data. Kahneman cites six such tendencies:

- **Substitution**. System 1 is prone to substituting a difficult question with a simpler one. In what Kahneman calls "the Linda problem," subjects of about an imaginary Linda, young, single, outspoken, and very bright, who, as a student, was deeply concerned with discrimination and social justice. They then asked whether it was more probable that Linda is a bank teller or that she is a bank teller and an active feminist. The overwhelming response was that "feminist bank teller" was more likely than "bank teller," violating logic (while every feminist bank teller is a bank teller, the

opposite is not true.) In this case, System 1 substituted an easier question – "Is Linda a feminist?" – and dropped the occupation qualifier.

- **Anchoring**. in which people's judgment is skewed by irrelevant data. The asking price of a home for sale will inevitably influence our estimation of the home's actual value, no matter how much we try to ignore that number.

- **Framing**. This is closely related to anchoring, because research shows that context can alter the way we respond to questions. In one study, for example, subjects were asked whether they would opt for surgery given a "survival" rate of 90 percent; others were asked the same question given a "mortality" rate of 10 percent. The positive context of the first question increased acceptance, even though the reality is that both outcomes are identical.

- **Availability bias**. This is a mental shortcut that occurs when people make judgments about the probability of events based on how easy it is to think of examples. For example, we are more likely to become concerned about airplane safety after reading about plane crashes in the news, or to worry about traffic fatalities after becoming aware of recent accidents. The problem is that the number of events that come to mind is not necessarily statistically equivalent to the probabilities of such events in real life.

- **Optimism and Loss Aversion bias**. Kahneman writes the illusion of overconfidence "may well be the most significant of the cognitive biases." When the mind makes decisions, it deals primarily with *Known Knowns*, phenomena already observed and understood; we rarely consider *Known Unknowns*, phenomena we know to be relevant but about which we have no information. And we are entirely unlikely to consider *Unknown Unknowns*, factors over which we have no control, including the potential effects of random luck.

- **The sunk cost fallacy**. Humans hate to admit defeat, and so are highly likely to continue to invest in efforts well after it's clear they won't work. This tendency to "throw good money after bad" leads us to continue investing in projects with poor prospects that have already consumed significant resources.

Thus, when executives complain about the quality of data or analytics this is often the result of the hard wiring of the brain, cognitive abilities and behavioral traits of the individual being expressed in the only way that it can be. This, in turn, tracks back to the BI and DS disciplines, or more specifically, to Quants' failure to understand the way the human brain makes decisions.

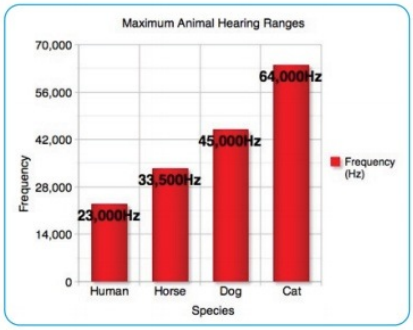
Next-generation decision Artificial Intelligence (HOAI) will be underpinned not by new data models, more interactive visual analytics or improved UI's. HOAI will begin the long journey to address the inherent limitations of human decision making from a Neuroscience, Cognitive and Behavioral Psychology perspective. This represents a fundamental shift in the way we approach problems such as Analytics at Scale. We have to get all the technical aspects correct from ingestion to the structure of the data lakes or warehouses, to the data models to selecting the appropriate visualizations – all of this must be correct. And then we must configure a new generation of dynamic multi-dimensional Artificial Intelligence that is capable of being decision maker centric and assisting to overcome the built-in deficiencies of human decision processes in strategic decision making. To be successful in this endeavor is to all but take the 'high ground' in any zero-sum or competitive game with a to fold advantage – to make better decisions through the avoidance of heuristic and psychological skew and to increase the speed of Ooda Loops. Analogies can be helpful in creating understanding. Think of this in fighter combat terms; HOAI will enable you to out climb and out turn your adversary in almost all situations. Now ask yourself – "what is that worth"?

The Coming Sixth Sense – Augmented Sensation

Decision making is partially predicated on sensing the environment. The capabilities of the sensing organs of a species is called by scientists The Umwelt.[6] This term denotes the sensory uniqueness of a species including human beings. For the blood-sucking tick, the umwelt is comprised of three biosemiotics (1) Oder (to smell appropriate animals to feed upon (2) Temperature (to identify an appropriate host through blood temperature (3) Hair topography (mammals only). Human beings have five identifiable senses, these are: Sight, Smell, Touch, Taste and Hearing. Yet as simple as this sounds from the perspective of decision analysis and building the next generation of decision AI we must go one level deeper.

[6] Is a German word for environment to denote an organism's sensory abilities.

We think we simply “see” or “hear” the world around us but this is not true. Our brain is taking photons of light and converting them through an extensive process into what we perceive – shapes, colors, etc. The same is true of hearing – you don’t simply hear the world as it is. The brain is taking air compression waves and converting them into what we perceive as sounds. These processes can even take place at differing speeds. Our auditory processes work faster than our visual cortex due to the size of the latter. And when the Umwelt is viewed by animal classification we realize that humans have very limited sensing of the ecosystem. A prime example of this is hearing; hearing differs greatly between species. The lesson to be learned is critical; we are fooled by the mind into believing we hear everything when we simply do not – not even close to everything!



Thus the question beckons - can human senses be augmented or entirely new senses are created to alter the human Umwelt in a way that radically improves strategic decision making? The answer to this question is Yes, through Augmented Sensation.

Initial experiments have revealed that if a stimulus such as sound or data is converted into dynamic patterns of sensation the brain will form new neural connections to interpret the new sensations. These new sensations can be a wearable device on the arm, back, etc. The conversion of data to dynamic patters to be sensed by the body can be done algorithmically from a device as simple as a tablet or phone. And, while early in its conceptualization development this vector shows tremendous promise in expanding the human Umwelt and as a result possibly improves situational awareness and decision making. The result from an organizational perspective could be massive. Imaging cyber data being sensed by a CISO or staff of experts in real-time. Imagine a new method of providing a Common Operating Picture of a military environment via felt data. The possibilities are endless as are the implications of such a technology becoming an operational reality.

Rear Admiral Enrique L. Arnaez es un oficial de guerra de superficie, armas de superficie y misiles. Tiene una Maestrías en Ingeniería de Control y Automatización de la Pontificia Universidad Católica del Perú y Política Marítima del Colegio de Guerra Naval del Perú. Fue nombrado Gerente de Proyecto para la creación del Comando de Defensa Cibernética de la Marina. Se ha desempeñado como Oficial de Enlace en el Comando de las Fuerzas de Flota de los Estados Unidos en Norfolk, VA, y Asesor del Presidente del Consejo de Delegados de la JID en Washington, DC. Actualmente es el Comandante del Comando de Defensa Cibernética Naval.

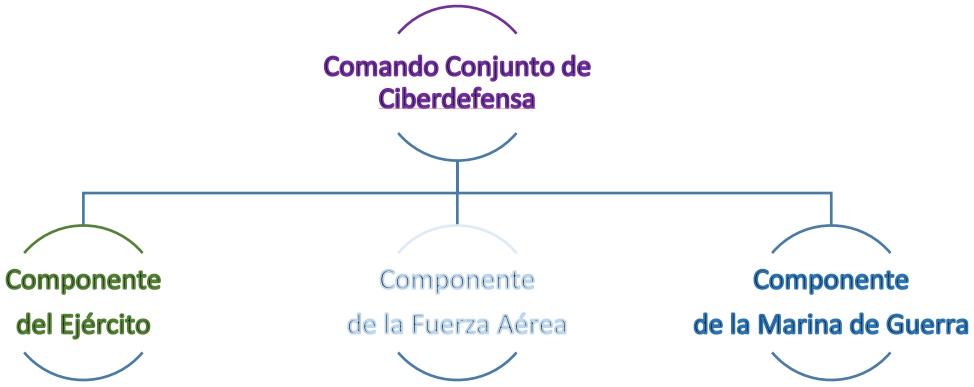
COMANDANCIA DE CIBERDEFENSA DE LA MARINA DE GUERRA DEL PERÚ

Introducción

Hoy en día la ciberdefensa ha tomado una gran importancia en las operaciones militares a nivel mundial, esto debido a las amenazas crecientes de ciberataques, no solo por parte de otros Estados sino también de individuos, grupos u organizaciones internacionales que buscan acceder a información confidencial o manipular sistemas de activos críticos de un estado o institución.

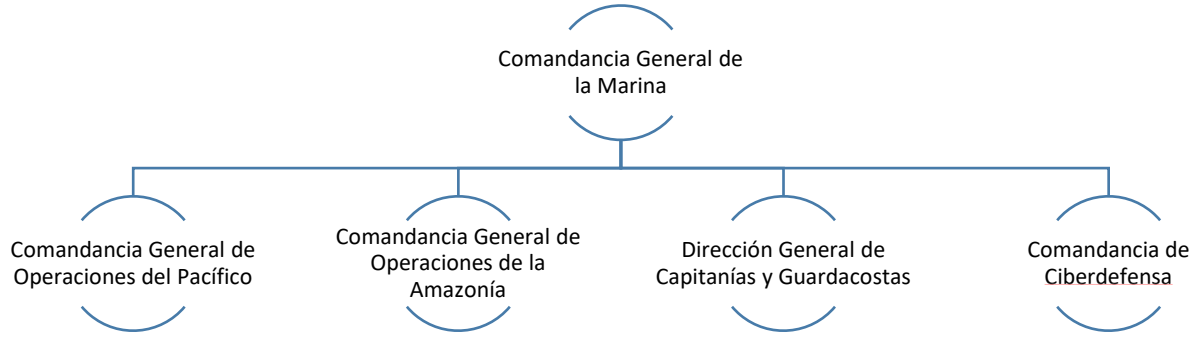
En ese aspecto, en el Perú se está creando un marco legal apropiado que ha comenzado con la Ley de Gobierno Digital y la Ley de Ciberdefensa, sus reglamentos están en un proceso de redacción y consulta que debe concluir en las próximas semanas, brindando una estructura de gobernanza y normativa que sea el sustento sólido para el desarrollo ordenado y robusto de las capacidades que toda Nación debe contar en el ciberespacio.

Por parte del sector Defensa, ya se tienen las directivas y planes que establecen la necesidad del desarrollo de la ciberdefensa nacional y el Comando Conjunto de las Fuerzas Armadas ha creado el Comando Conjunto de Ciberdefensa (COCID), y ha formulado la Doctrina Conjunta de Ciberdefensa.



Así mismo, ha conducido su primera operación a través de sus componentes ciber de la Fuerza Aérea, de la Marina de Guerra y del Ejército, orientada a la defensa de la infraestructura crítica nacional durante los Juegos Panamericanos Lima 2019, disponiendo que la Comandancia de Ciberdefensa de la Marina se encargue específicamente de la Ciberdefensa de la Infraestructura Deportiva de los Juegos mencionados.

Derivando al tema del artículo sobre el desarrollo de la ciberdefensa en la Marina de Guerra del Perú, es bueno comenzar señalando que la Comandancia de Ciberdefensa de la Marina de Guerra del Perú (COMCIBERDEF), tiene como misión asegurar las operaciones en el dominio del ciberespacio, manteniéndolo seguro para el uso de las propias fuerzas navales. Esta comandancia lleva más de un año realizando operaciones en el ciberespacio, siendo la cuarta fuerza operacional de la armada, al mismo nivel que la Comandancia General de Operaciones del Pacífico, Comandancia General de Operaciones de la Amazonía y la Dirección General de Capitanías y Guardacostas debido a que es un dominio distinto y demanda capacidades nuevas.



COMCIBERDEF viene efectuando las tareas de defender activos propios mediante el monitoreo permanente del flujo de información detectando intentos de ataques, evaluando y analizando cualquier riesgo informático, coordinando y ejecutando operaciones defensivas en caso de algún ataque, y, si fuese necesario, respondiendo lo antes posible para asegurar el uso irrestricto del ciberespacio, siempre bajo le observancia irrestricta del cumplimiento de la ley.

En tal sentido para lograr el cumplimiento de estas tareas se tienen en consideración dos factores, el aspecto humano y tecnológico. Para esto se cuenta con personal calificado, capaz de desenvolverse en cualquier campo de las operaciones en el ciberespacio; en referencia al aspecto

tecnológico, estamos siempre en la búsqueda de nuevas herramientas, así como de la actualización de nuestros sistemas existentes y equipo especializado.

Como está organizada la Comandancia de Ciberdefensa

La Comandancia de Ciberdefensa de la Marina es un órgano de línea de la Comandancia General de la Marina y, en caso de operaciones militares, es el componente naval del Comando Conjunto de Ciberdefensa (COCID).

La Comandancia de Ciberdefensa de la Marina consta actualmente de tres departamentos para las diferentes operaciones:

- Departamento de Operaciones de Defensa, encargado principalmente de monitorear todas las redes de la armada para minimizar los incidentes informáticos.
- Departamento de Explotación, encargado de la búsqueda de amenazas para el empleo del ciberespacio en base a información de fuente abierta a nivel local y global.
- Departamento de Operaciones de Respuesta, responsable de contraatacar cualquier amenaza.

Capacidades Operacionales de la Comandancia de Ciberdefensa

Asimismo, cuenta con una sección dentro de su estado mayor llamada Investigación Digital, la cual está encargada de realizar el análisis forense informático, ingeniería reversa e investigación y desarrollo de nuevas tecnologías.

Las amenazas y cómo las afrontamos

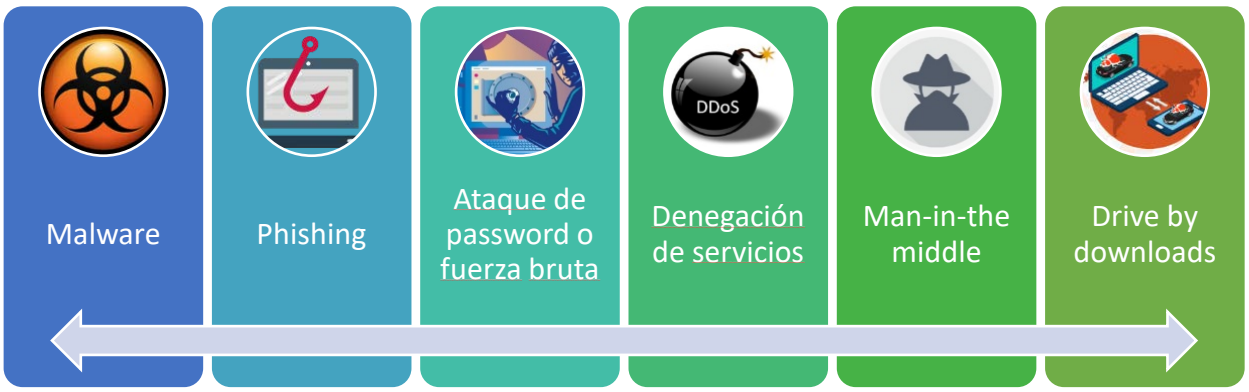
Las amenazas son diversas, desde jóvenes que pretenden entrometerse en el ciberespacio de la Marina de Guerra, hasta las organizaciones internacionales que tratan de robar información clasificada o producir algún daño en nuestros sistemas, sin dejar de ver a los cibercriminales comunes o a posibles actores estatales maliciosos.

Entrando un poco al detalle, uno de los tipos de ataque que representa una de las mayores amenazas hoy en día, son los ataques de "ransomware", que es un tipo de malware cuyo fin es encriptar archivos dentro de una red, denegando el acceso de los usuarios al sistema o información secuestrados, hasta que se cumpla con un pago, normalmente a una cuenta intrazable o simplemente para dejarlos encriptados.

Entrando más en el ámbito naval, otros tipos de software maliciosos a los que se puede ser vulnerable son aquellos que pueden poner en peligro los sistemas de comando y control de las unidades navales, como por ejemplo lograr penetrar algún aplicativo o herramienta periférica para alterar o impedir su correcto funcionamiento, desorientando o manipulando el comportamiento del buque.

Sin embargo, una grave amenaza que usualmente no es considerada, es la falta de conciencia y desinterés del personal, en cuanto a ciberseguridad y ciberdefensa; esto ha conllevado a idear un ambicioso programa para mejorar el comportamiento del factor humano en esta área.

"*Todas las cadenas son tan fuertes como su eslabón más débil"*. En el caso del ciberespacio, los componentes de la cadena son el hardware, con el WiFi incluido, el software, y las personas, quienes son las que interactúan con los teclados, los DVDs y CDs, con los mouses, los pendrives y también quienes hacen clic donde no deben y permiten el accionar de las amenazas. Mientras los usuarios no nos sintamos como parte del ciberespacio al interactuar con él, este será el eslabón más débil y por donde los ataques se realizarán.



Para atender esta falta de conciencia señalada en los párrafos anteriores, COMCIBERDEF constantemente protege a las redes de la armada mediante una arquitectura de red segura con sistemas confiables, los que mitigan incidentes informáticos y descartan los falsos positivos que normalmente ocurren durante las operaciones diarias. En esta vigilancia permanente, se coloca especial atención al comportamiento de los usuarios ya que son el eslabón más débil de la estructura de ciberdefensa.

Capacitación y Entrenamiento

Para lograr el cumplimiento de la misión y tareas se han desarrollado programas dirigidos a proteger las redes y capacitar al personal a operar en el complejo dominio del ciberespacio. Todo el personal naval necesita cierto grado de entrenamiento en este campo, pero no todos requieren el mismo nivel de instrucción, en tal sentido se han desarrollado diferentes tipos de entrenamientos acordes a cada uno de estos niveles, siendo responsable el comando de identificar al personal que requiere capacitación especializada en ciberseguridad, dependiendo del rol que cumple dentro de la institución.

Es por este motivo que es necesaria la mejora e incremento de las capacidades de ciberdefensa, por lo que se ha considerado el próximo año la ampliación de las instalaciones de la comandancia, con la finalidad de distribuir mejor al personal y equipamiento asignado, así como incrementar las capacidades del centro de datos.

Experiencias trasladadas

Desde la creación de la comandancia, la Comandancia de Ciberdefensa ha participado en diferentes simposios y conferencias, tales como el Simposio de Ciberdefensa en la JID en el 2018, Simposio Internacional de Defensa de la Escuela Superior de Guerra Naval en el 2018 y 2019, Conferencia de Ciberdefensa del Hemisferio Oeste en Bogotá, Colombia en el 2019 entre otras, las cuales han permitido entender e identificar las limitaciones y brechas de las capacidades actuales y los requerimientos necesarios para llevar a cabo operaciones en el ciberespacio en todo nivel.

Del mismo modo, se realizan constantemente operaciones a nivel institucional con la participación de unidades navales y dependencias de tierra para asegurar el uso irrestricto del ciberespacio por parte de los usuarios de la red.

Juegos Panamericanos y Parapanamericanos Lima 2019

Asimismo, en los meses de julio, agosto y setiembre de este año se realizaron en la ciudad de Lima los Juegos Panamericanos y Parapanamericanos Lima 2019, para los cuales COMCIBERDEF tuvo una participación destacada en apoyo a la ciberdefensa de los sistemas informáticos deportivos de este evento internacional, aportando en la implementación, desarrollo y configuración del sistema de gestión de eventos e información de seguridad (SIEM).

El centro de operaciones de seguridad, mejor conocido como SOC, de los Juegos Panamericanos, fue concebido, diseñado, dotado operado en coordinación con los responsables de tecnologías de información de la organización de los Juegos Panamericanos, y fue implementado

completamente como un segundo nivel de ciberseguridad para el control de todos los activos informáticos y servicios web que habían sido contratados para tal fin.

Para tal efecto, la Comandancia de Ciberdefensa de la Marina, destinó personal idóneo, quien estuvo monitoreando y analizando en este segundo nivel de seguridad, todos los sensores y herramientas instalados durante las 24 horas del día desde el inicio hasta el término de los juegos.

Cabe resaltar, que la integración con los proveedores de los servicios, así como con lo proveedores del mantenimiento de la infraestructura informática fue muy estrecha permitiendo que absolutamente todos los intentos de ataque producido durante los juegos panamericanos sean bloqueados.

Para seleccionar el mejor escenario o alternativa de acción, se sostuvieron reuniones que trasladen las lecciones aprendidas por el Reino Unido en las Olimpiadas de Londres, y especialmente Brasil en los Juegos Olímpicos de Río de Janeiro y la Copa del Mundo de Fútbol.

A estas experiencias compartidas, se debe agregar que la implementación de la Comandancia de Ciberdefensa de la Marina fue parte del mismo proceso para la defensa de los Juegos Panamericanos Lima 2019, ya que el mismo personal entrenado en operaciones y en recibir la tecnología fue el encargado de replicar los sistemas correspondientes en el Centro de Operaciones de Seguridad de los Juegos.

Adicionalmente, vale decir que las Operaciones de Los Juegos Panamericanos aceleraron el desarrollo de nuevos procedimientos y conceptos doctrinarios basados en experiencia.

El resultado fue que pudimos mantener todos los sistemas y redes involucradas disponibles, confiables y seguras a pesar de ciberataques de DoS, DDoS, intentos de penetración, infecciones

de virus y hasta ransomware que ocurrieron durante los juegos, siendo estos neutralizados en el menor tiempo posible.

Coordinación, cooperación y resiliencia

Es fundamental en este nuevo dominio del ciberespacio, tener la certeza de que nadie puede avanzar solo ante las nuevas amenazas que en él se encuentran.

Es por ese motivo, que la colaboración y la cooperación entre organizaciones públicas y privadas sean tanto nacionales como internacionales, es crucial para asegurar el correcto empleo este dominio y dárselo a todos los actores hostiles y criminales que se encuentran en el.

Sino que debemos también actuar con resiliencia para estar preparados ante nuevas situaciones que puedan afectar a la ciberseguridad en este nuevo dominio.

Estas condiciones de cooperación, colaboración y resiliencia con los diferentes organismos del Estado vinculados al empleo de tecnologías digitales, de la Internet, de servicios que puedan afectar la identidad de los ciudadanos, y hasta el mismo sistema financiero, deben ser alcanzadas con organizaciones estatales, con la academia, con el sector privado, y con la industria, así como organizaciones internacionales para lo cual es una necesidad establecer canales rápidos de intercambio de información útil.

Esta información a la que nos referimos comprende a las Alertas, que se refiere a los ataques que están sucediendo en alguna de nuestras organizaciones Y que podría ampliar su objetivo hacia nosotros, a las amenazas, que son los grupos de interés desde donde se podría en el futuro gestionar un ataque, y a las Vulnerabilidades, que son las fallas de seguridad que reportan los fabricantes de hardware y software por donde un ciberdelincuente podría atacar a su objetivo.

El método más conocido para el intercambio de esta información es conocido como centros de respuesta a emergencias de seguridad, o simplemente CERT o CSIRT, por sus siglas en inglés. Estos centros facilitan el intercambio Y la conectividad entre todos los afiliados.

Mientras más organizaciones participamos en este tipo de centros, más protegidos vamos estar contra las amenazas en el ciberespacio.

Conclusiones

Si bien es cierto, Comandancia de Ciberdefensa es una comandancia joven en relación a otras dentro de la Marina de Guerra del Perú, las experiencias ganadas en este corto tiempo y el compromiso de su dotación la han hecho una de las más reconocidas a nivel nacional en el campo de la ciberseguridad y ciberdefensa, asesorando a instituciones estatales y privadas, aportando su conocimiento en beneficio del desarrollo nacional.

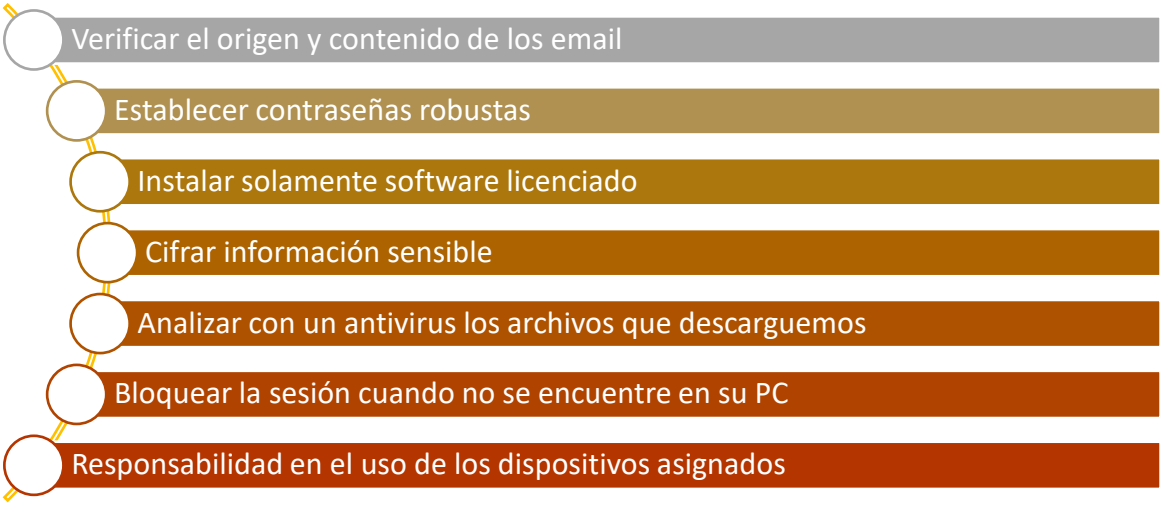
La colaboración y cooperación en el entorno de la seguridad digital, ciberseguridad y ciberdefensa, es un elemento primordial, tanto en entre organizaciones públicas como privadas, nacionales y extranjeras, ya que solos, nadie va a poder estar seguro.

La concientización de los usuarios de los sistemas informáticos y operativos debe ser reforzada, practicada y evaluada permanentemente para minimizar vulnerabilidades de factor humano que son los más frecuentes.

La libertad y seguridad en el ciberespacio es una tarea difícil que nos compromete a todos para poder mantener la confidencialidad, integridad y disponibilidad de nuestra información dentro de un dominio difuso, sin fronteras y permanentemente acechado por intereses adversos a los nuestros.

Recomendaciones para trabajar en un ambiente seguro

Este es el listado de buenas costumbres que cualquier usuario debe considerar para trabajar en un ambiente seguro:



Escudo y heráldica de la Comandancia de Ciberdefensa de la Marina de Guerra del Perú

El Escudo representa un tridente que sale del mar y se orienta al Sol.

El mar está conformado por un código hash que dice "*Defensa de los intereses Nacionales en el Ciberespacio*", seguido de un código binario que dice "*Comandancia de Ciberdefensa*".

El tridente es una representación modificada de una manifestación pre-Inca del Candelabro Paracas. El diente de la izquierda con forma de escudos intenta representar a las operaciones de

Defensa, el diente central representa la búsqueda de las amenazas de las Operaciones de Explotación y el diente de la derecha con sus flechas a las Operaciones de Respuesta.

El Sol, que es una deidad de muchas de las culturas precolombinas peruanas, es nuestra misión.

Por último, el lema "*Malo mori quam foedari*", quiere decir prefiero morir antes que mancharme, lo que éticamente podría decirse que es "*Prefiero morir antes que la deshonra*"

Capitán de Fragata Pablo Ramón Mercado Hernández tiene Maestría en Seguridad de la Información Centro de Estudios Superiores Navales de la Secretaría de Marina, Maestría en Administración de Tecnologías de la Información. Especialidad en Seguridad Informática y Tecnologías de la Información. Línea de investigación: Seguridad en Infraestructura. Ciberseguridad y Ciberdefensa. Es Catedrático en el Centro de Estudios Superiores Navales. Actualmente es el Subdirector de Investigación y Desarrollo Unidad de Ciberseguridad (Uniciber) de la Secretaría de Marina de México.

CIBERSEGURIDAD Y CIBERDEFENSA:
MEJORES PRÁCTICAS Y LECCIONES APRENDIDAS

> "Vamos a ser una institución siempre presente y resuelta a apoyar a su pueblo. Defensora y respetuosa de la ley, de los derechos humanos, y de la justicia. Una Marina que hoy, hace suyos los ideales de toda nuestra nación".
> Almirante José Rafael Ojeda Durán, Secretario de Marina
> Discurso de Entrega-Recepción, 1-Dic-2018

I. Misión

La Armada de México, tiene la misión de emplear el Poder Naval de la Federación para la defensa exterior y coadyuvar en la seguridad interior del país; en los términos que establece la Constitución Política de los Estados Unidos Mexicanos, las leyes que de ella derivan y los tratados internacionales. La visión de la Marina de México, es la de ser una Institución que coadyuve a lograr las condiciones de paz y desarrollo de la Nación, indispensables para la construcción de un país próspero y con responsabilidad global, empleando el Poder Naval de la Federación, fortaleciendo sus capacidades de respuesta operativa, consolidando la inteligencia naval, modernizando procesos, sistemas e infraestructura, impulsando la investigación, desarrollo tecnológico y la industria naval.

Con estas premisas estrechamente relacionadas con la modernización y empleo de tecnologías, tras un largo desarrollo que inicia en el año de 2004, la Marina de México consolida la Ciberdefensa y Ciberseguridad mediante un Acuerdo Secretarial, el número 033 del día 13 de febrero de 2017, donde se crea la Unidad de Ciberseguridad del Estado Mayor General de la Armada, con la misión de planear, conducir, y ejecutar actividades de seguridad de la información, ciberseguridad y ciberdefensa para la protección de la infraestructura de información de la Secretaría de Marina-

Armada de México (SEMAR) y coadyuvar en el esfuerzo nacional para el mantenimiento de la integridad, estabilidad y permanencia del Estado Mexicano.

Para comprender la evolución de la Ciberdefensa, Ciberseguridad y Seguridad de la Información en la Marina de México, es necesario contextualizar los conceptos que se manejan en el tema, en el ámbito de información y del Ciberespacio, así como el desarrollo histórico de la Unidad dentro de la organización.

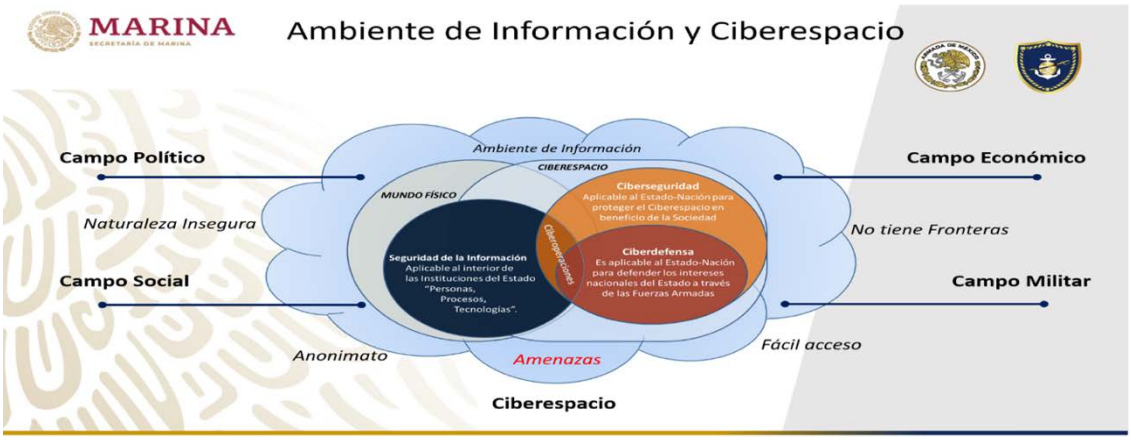
II. Ciberseguridad y Ciberdefensa

Del Glosario de la Estrategia Conjunta de Ciberdefensa SEDENA-SEMAR, se desprenden los conceptos de **ciberdefensa**, como la capacidad del Estado Mexicano para realizar acciones de seguridad y defensa nacional en el Ciberespacio, y el concepto de **ciberseguridad**, como el conjunto de controles, procedimientos y normas del estado para proteger y asegurar sus activos en el Ciberespacio.

La Ciberseguridad se propicia a través de una condición de protección y aseguramiento, mientras la Ciberdefensa denota una acción o conjunto de acciones para resguardar esa condición en el Ciberespacio para los mexicanos.

III. Ambiente de Información y Ciberespacio

Las sociedades interactúan en un ambiente de información físico y cognitivo, en el entorno digital denominado Ciberespacio, conceptualizado como el ámbito intangible, de naturaleza global, soportado por las tecnologías de información y comunicaciones, que es utilizado para la interacción entre individuos y entidades públicas - privadas.

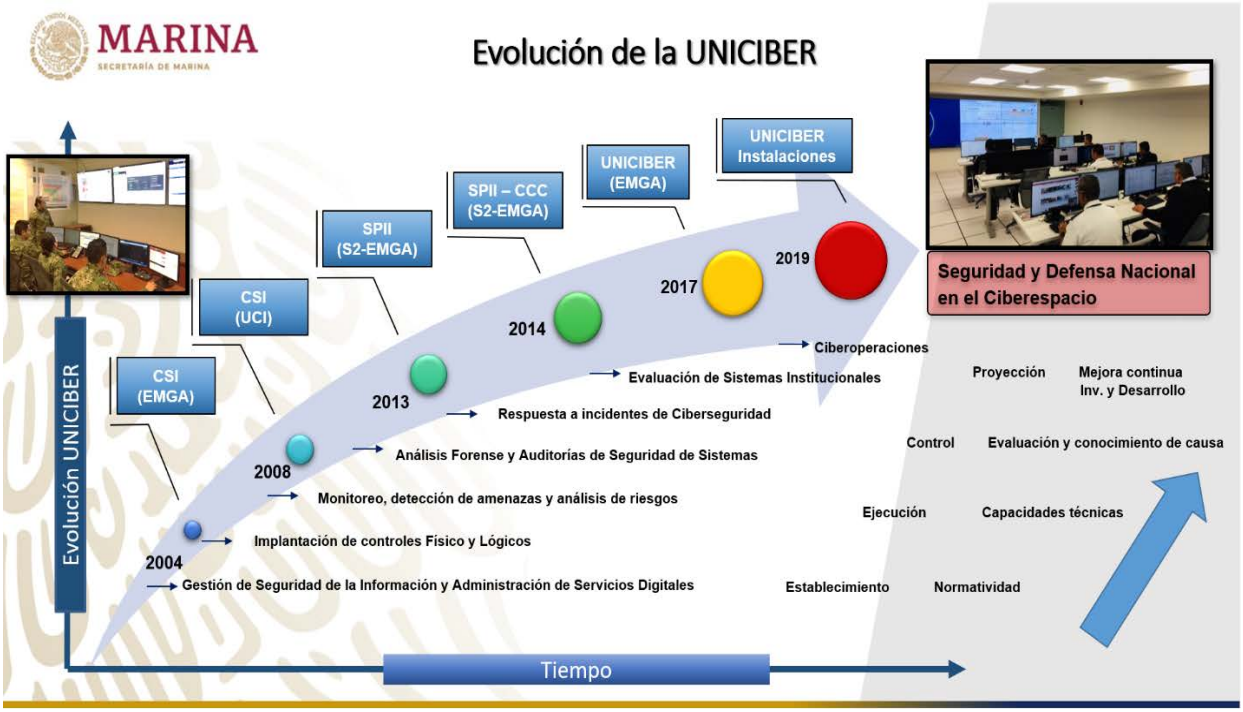


En ese entorno virtual, se identifican múltiples beneficios en los campos político, económico, social y hasta militar, pero se advierten riesgos para los Estados por la naturaleza insegura, la falta de fronteras, así como el anonimato y facilidad de acceso a recursos a bajo costo por un agente amenaza. La Unidad de Ciberseguridad, como parte de sus atribuciones tiene la de construir y mantener fuerzas y capacidades para planear y conducir operaciones en el Ciberespacio, por lo cual con una visión integral, identificó que se requiere mantener acciones de seguridad de la información, de Ciberseguridad y de Ciberdefensa, por si mismas o en apoyo a las operaciones en las otras dimensiones (mar, aire, tierra, espacio), en estricto apego y respeto a los derechos humanos, a la transparencia y a la disposiciones jurídicas aplicables a nivel nacional e internacional.

En este aspecto, cabe destacar en el tema que ocupa al presente escrito, que con la creación de la Unidad en 2017 y como parte de sus atribuciones, se tuvieron que desarrollar los principios de la Estrategia Institucional de Ciberseguridad y Ciberdefensa, por lo que basados en la experiencia de 13 años, se identificó que la buena práctica de realizar análisis de riesgos como punto de partida para realizar actividades de ciberseguridad, como lo marcan la mayoría de estándares, normas y buenas prácticas en el tema, requirió ser fortalecida con metodologías de planeación estratégica estableciéndose así la necesidad de desarrollar análisis de Fortalezas, Oportunidades, Debilidades y Amenazas, Análisis Coyunturales y Prospectivos, entre otros, con la finalidad de presentar al Mando elementos de juicio, completos e integrales, para la toma de decisiones en el corto, mediano y largo plazo.

IV. Evolución

La Ciberseguridad en la Marina de México, obedece a un conjunto de hitos que han marcado su derrotero en el desarrollo organizacional y que le dan sentido a la forma de desarrollar sus actividades.



El 16 de Julio de 2004, en Acuerdo Secretarial, se crea la Comisión de Seguridad de la Información de la Armada de México, como parte integrante del Estado Mayor General, con los objetivos principales de garantizar la confidencialidad, integridad y disponibilidad de la información, establecer gobernabilidad de seguridad en la administración de servicios digitales, mediante un sistema integral basado en las mejores prácticas nacionales e internacionales.

Entre 2004 y 2008, se consolida la implantación de controles físicos y lógicos, se desarrollan 47 de los 88 documentos rectores en el tema como son políticas, directivas, doctrina, guías y manuales que comprenden aspectos de clasificación, áreas de protección, sistemas de cifrado, políticas de uso de internet, de seguridad de redes, de seguridad en las personas, de contraseñas, de manejo de pruebas digitales, de seguridad física, de uso de dispositivos de almacenamiento removibles, entre otros.

De manera coordinada, con fecha 16 de junio de 2005, se crea la Maestría en Seguridad de la Información, primera en su tipo en América latina, adscrita al Centro de Estudios Superiores Navales de la Universidad Naval de México, el posgrado tiene como objetivo formar personal altamente capacitado para la investigación, el diseño y la implementación de sistemas informáticos seguros, con conocimientos de los principales estándares de seguridad, capaz de realizar pruebas de reconocimiento y evaluación de riesgos potenciales y con propuesta de solución a problemas reales.

En las aulas del Centro de Estudios Superiores Navales, se han formado desde esa fecha 134 Maestros en Seguridad de la Información, de los cuales el 30% aproximadamente son personal civil que labora en las dependencias de la Administración Pública Federal, lo cual ha permitido divulgar a nivel gobierno la preocupación de la Institución en el tema, establecer un marco de cooperación interpersonal, además de contribuir a la solución de problemáticas reales, al incluir entre otras actividades, la realización de investigación con temas de tesis y de proyectos de desarrollo tecnológico basados en problemáticas reales, así como la interacción directa con el área encargada de la Ciberseguridad de la Marina.

En 2008, ante la necesidad de implementar técnicamente la normatividad que se había venido consolidando, la Comisión de Seguridad de la Información, pasó a depender de la Unidad de Comunicaciones e Informática, desarrollando y fortaleciendo las capacidades técnicas de monitoreo, detección de amenazas y de análisis de riesgos.

En 2013, una vez fortalecidas las áreas técnicas, se inicia el despliegue de capacidades operacionales y tácticas, reincorporando la entonces Comisión de Seguridad de la Información a la Sección de Inteligencia del Estado Mayor General, como Subsección de Protección de Infraestructuras de Información, incrementándose las capacidades de Análisis forense, peritaje informático, auditoría de sistemas y de respuesta a incidentes de ciberseguridad.

Finalmente, en 2017, sin dejar de pertenecer al Estado Mayor General, se crea la actual Unidad de Ciberseguridad, dotándola de nuevas instalaciones e incrementando las capacidades tecnológicas y humanas, que le permitirán a la Institución el desarrollo de Ciberoperaciones. Para lo cual, se han desarrollado mayores capacidades para realizar auditoría de sistemas, análisis de código malicioso, ingeniería inversa, evaluación de ciberseguridad de sistemas y aplicativos de cómputo, minería de datos, ciberinteligencia y planeamiento naval operativo.

En estos aspectos como parte del tema que ocupa al presente escrito, las buenas prácticas indican Planear antes de Ejecutar (Ciclo Deming), sin embargo las lecciones aprendidas indicaron que en la evolución “no sobrevive el más fuerte, sino el que se adapta” (Darwin, 1859), de tal forma que en la Institución, la adaptabilidad y resiliencia permitieron a la seguridad de la información evolucionar hacia la ciberseguridad y ciberdefensa, sentando las bases para crear la capacidad de desarrollar ciberoperaciones en el futuro cercano.

V. Instalaciones de la Unidad de Ciberseguridad

Las nuevas instalaciones asignadas a la Unidad en 2019, se encuentran dentro de un Polígono Naval donde se ubica el Centro de Estudios Superiores Navales (CESNAV), con cuya Dirección se vienen desarrollando una serie de vinculaciones académicas que incluyen: investigación, realización de seminarios, prácticas, orientación y asesoría en la elaboración de temas de investigación de tesis.

La Universidad Naval se ha preocupado por mantener actualizado el plan de estudios de la Maestría de Seguridad de la Información conforme a las necesidades de formación de personal, además ha incluido asignaturas optativas de Ciberseguridad para los distintos posgrados que se imparten en el Centro, desarrollando de forma alternada desde 2015, ejercicios de crisis cibernética como parte del entrenamiento en asignaturas relacionadas con planeamiento naval operativo. Como caso de éxito, se destacan trabajos de investigación tipo tesis concluidas por discentes de posgrado del CESNAV, con temas propuestos por la Unidad de Ciberseguridad, que materializan la participación de la Universidad Naval en la solución de problemas reales, como es el caso de la Gestión de riesgo cibernético en el ámbito marítimo y portuario, producto académico que aporta a la Institución propuestas para las modificaciones a leyes, el establecimiento de normas oficiales mexicanas y planes de capacitación para dar cumplimiento a requerimientos internacionales sobre

seguridad, la protección marítima y portuaria y el comportamiento ambiental que ha de observarse en el transporte marítimo internacional, a implementar como Autoridad Marítima Nacional.

Al respecto de buenas prácticas de colaboración con el sector gobierno, sector privado y sector académico en el tema de ciberespacio, las lecciones aprendidas como lo indican los resultados, muestran un sector académico con mayor disposición para colaborar en comparación con los otros sectores, por la situación privilegiada en México, de contar con universidades de alto prestigio de carácter público y desarrolladas con fondos del Estado.

VI. Organización

La Unidad de Ciberseguridad, está conformada por cuatro Direcciones de área: de Ciberdefensa, de Ciberseguridad, de Gestión de Seguridad de la Información y de Investigación y Formación, así como un Departamento de Autoridad Certificadora de firma digital, con funciones específicas en cada campo, además se cuenta con un Centro de Ciberdefensa y Ciberseguridad, en el cual a través de una organización transversal y multidisciplinaria se conducen operaciones en el ciberespacio para proteger las infraestructuras críticas de información de la Secretaría de Marina Armada de México, conformada por dos células de operación con funciones de detección, monitoreo, respuesta, control y seguimiento.

Entre las actividades que se desarrollan en el centro están las de exploración de amenazas, monitoreo de redes institucionales y de redes críticas, investigación, respuesta, control y seguimiento

de incidentes, coordinaciones internas y externas. Se cuenta con plataformas de intercambio de información con otros Centros de Respuestas a Incidentes Cibernéticos nacionales e internacionales, participación en el Foro Iberoamericano de Ciberdefensa y de la plataforma MISP (Malware Information Sharing Platform).

En aspectos de organización, las buenas prácticas indican el establecimiento de la función de seguridad, con delimitación de roles y responsabilidades; en las lecciones aprendidas, la Institución ha desarrollado la capacidad de realizar trabajo colaborativo y coordinado, estableciendo grupos multidisciplinarios que atienden con el nivel de especialidad y profundidad suficiente, los asuntos que se requieran.

VII. Capacidades Operativas

En cuanto a diseños de arquitecturas de ciberseguridad, las buenas prácticas recomiendan el empleo de seguridad en capas, o en profundidad, lo cual comúnmente se interpreta y relaciona con controles tecnológicos en la infraestructura; las lecciones aprendidas han permitido identificar que las capas de seguridad deben establecerse y conformarse con personas, procesos y tecnologías.

Por lo anterior, en la infraestructura crítica de información de la Marina, se adoptó una arquitectura de seguridad en capas, en las que interactuando con la Unidad de Ciberseguridad, se involucra en tareas de seguridad al usuario final como primer respondiente ante incidentes, pasando por el administrador de red, el oficial de seguridad de la información, las direcciones de soporte de

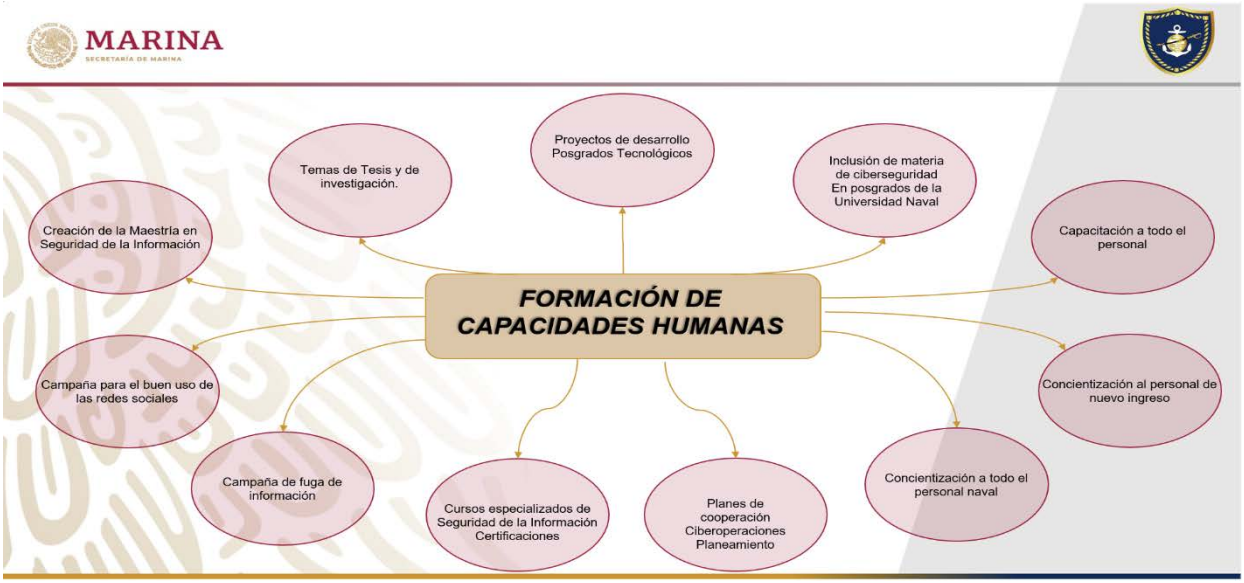
tecnologías hasta llegar a esta Unidad, coadyuvando de ser necesario con el área de ciberinteligencia, y otras áreas no tecnológicas como las de comunicación social, aspectos legales, de transparencia y acceso a la información pública, de protección de datos personales, etc. según la situación lo amerite, todo ello para generar información de alto nivel para tomadores de decisiones. Las lecciones aprendidas permitieron el desarrollo de Protocolos de actuación ante incidentes en el Ciberespacio, así como boletines técnicos que permiten mantener sanos los sistemas institucionales.

VIII. Capacitación y Entrenamiento

La Marina a través de acuerdos internacionales de Cooperación con otras Fuerzas Armadas, como por ejemplo las de los EE.UU. han llevado a cabo diversos ejercicios combinados en ciberseguridad desde el año 2015.

El propósito ha sido desarrollar un entendimiento mutuo en roles militares y la generación de doctrina, con el fin de lograr una interacción a nivel operativo y táctico, por medio del intercambio de expertos y de entrenamientos que han permitido fortalecer las capacidades y destrezas de los participantes. Se pueden citar ejemplos como los ejercicios Ciber Libertad 2015, Ciber Libertad de las Américas 2016, Ciber Libertad de las Américas 2017, Ciber Tradewinds 2018 y Ciber Cays 2019. Además de la participación en otros entrenamientos como CyberWoman Challenge, HackMex del Instituto Politécnico Nacional y otros de captura de bandera.

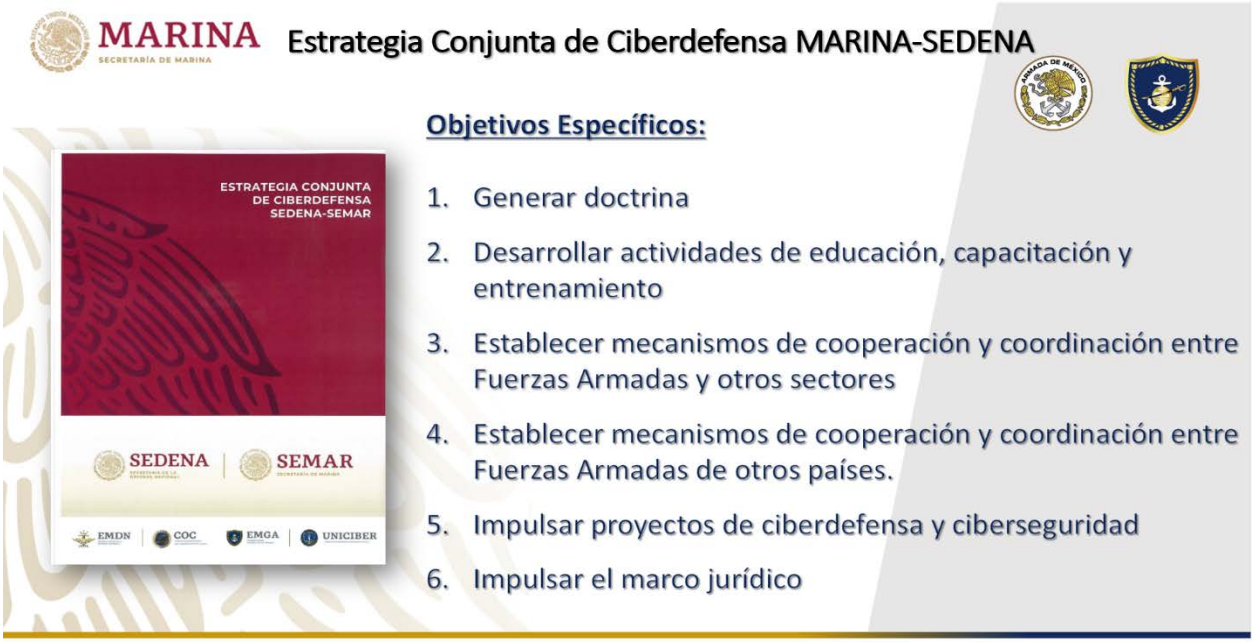
Las buenas prácticas de cooperación y entendimiento, están en desarrollo, dejando como lecciones aprendidas, la necesidad de crear doctrina en materia de ciberoperaciones y generar procedimientos para respuesta oportuna; empleando pensamiento lateral crítico y analítico, para considerar el peor y el mejor escenario, complementando lo tradicional con reingeniería e innovación, buscando la convergencia de enfoques descendentes y ascendentes, con lo cual se ha ampliado el panorama de los expertos de la unidad para la solución de problemas.



IX. Normatividad

Como parte fundamental de los compromisos establecidos como objetivo de cooperación, entendimiento e intercambio de información la Secretaría de Marina Armada de México (SEMAR) desarrolló con el Centro de Operaciones del Ciberespacio de la Secretaría de la Defensa Nacional (SEDENA-COC) la Estrategia Conjunta de Ciberdefensa SEDENA- SEMAR, para establecer las acciones de las Fuerzas Armadas Mexicanas en materia de ciberdefensa, para permitir generar capacidades y proteger la infraestructura de tecnologías de información y comunicaciones propias, y coadyuvar a la Seguridad y Defensa Nacional ante amenazas y/o ataques cibernéticos, con la visión de que las Fuerzas Armadas Mexicanas sean capaces de garantizar la Seguridad y Defensa Nacional en el ciberespacio con pleno respeto a los derechos humanos. Por otro lado, se ha participado en la elaboración de la Estrategia Nacional de Ciberseguridad, en la Elaboración de la Propuesta de adición al Código Penal Federal y Ley de Seguridad Nacional para la elaboración del marco jurídico

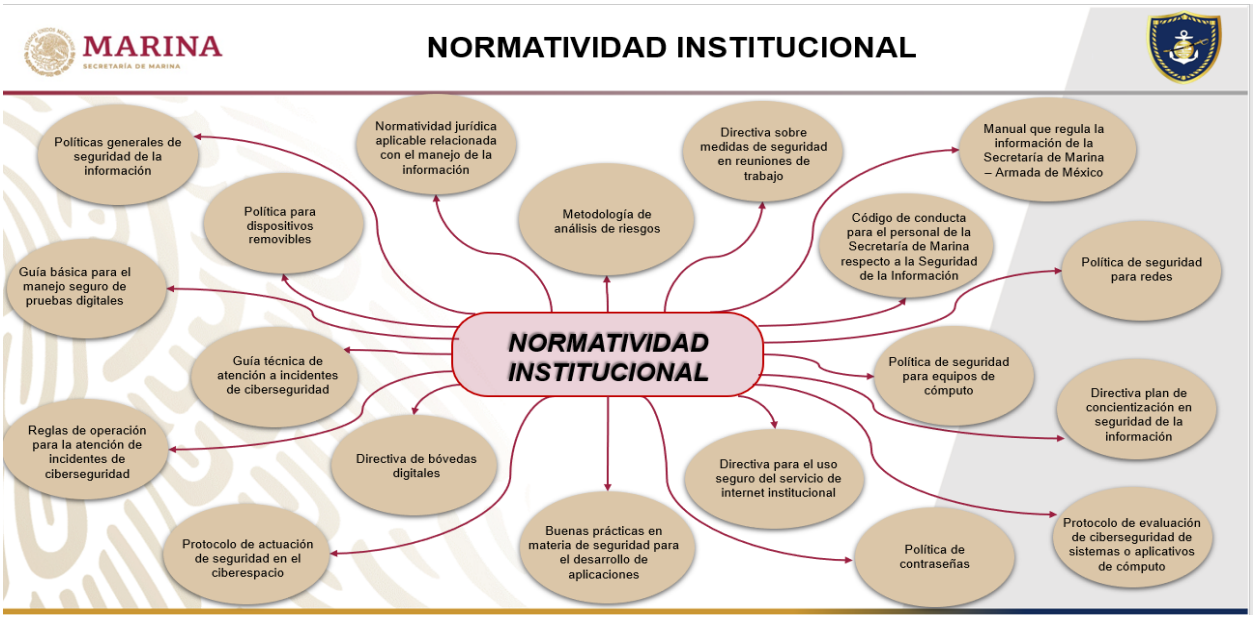
que dé sustento legal a la actuación de las Fuerzas Armadas en el Ciberespacio, en la elaboración del Manual Administrativo de Aplicación General en materia de Tecnologías de Información Comunicaciones y Seguridad de la Información (MAAGTICSI), promoviendo el desarrollo de normatividad en bien de la seguridad del ciberespacio para los mexicanos.



Por otro lado en base a sus funciones de la Unidad de Cibereseguridad, se han desarrollado, difundido e implementado cerca de 100 documentos normativos, entre ellos se pueden citar las Reglas de Operación para la atención de incidentes de ciberseguridad, el Protocolo de Actuación de Seguridad en el Ciberespacio, la Guía Técnica de Atención a Incidentes de Ciberseguridad, los cuales guardan relación al establecer los roles y responsabilidades a nivel estratégico, operacional y táctico para la atención de incidentes en el ciberespacio.

Actualmente la Institución se encuentra en proceso de desarrollo de normatividad relativa al riesgo cibernético en el ámbito marítimo y portuario. A partir de las Directrices MSC-FAL 1/Circ. 3 del 5 de julio de 2017, sobre la gestión de riesgos cibernéticos marítimos y la Resolución MSC.428(98) emitida el 16 de julio de 2017 por la Organización Marítima Internacional y estados miembros, en donde se alienta a que se aborde la gestión de riesgos cibernéticos marítimos como parte del Código Internacional de Gestión de Seguridad (IGS); para integrarse en las verificaciones que se realizarán, a partir del 1 de enero de 2021. Lo anterior plantea un reto a la Marina, para generar propuestas de adecuaciones a la ley de Navegación y Comercio Marítimo, así como el

desarrollo de una norma oficial que permita la certificación y la inspección en el tema, lo anterior a raíz de que el poder ejecutivo federal ejerce la Autoridad Marítima a través de la Secretaría de Marina, para garantizar que se cumpla con la legislación aplicable en la materia, integrando en un binomio las atribuciones de las Capitanías de Puerto y los medios con los que la Secretaría de Marina ejerce las funciones de Guardia Costera.



Las buenas prácticas en el tema dejan lecciones aprendidas a la Institución, en las cuales toda actividad debe contar con el sustento legal y normativo, por lo que en el ámbito de su competencia siempre promueve los mecanismos para lograrlo.

X. Conclusiones

Las buenas prácticas son un punto de referencia excelente que enriquecen el planeamiento y desarrollo de actividades de ciberseguridad y ciberdefensa por instituciones militares, las cuales deben retroalimentarse con las lecciones aprendidas. El esfuerzo académico realizado por el Colegio Interamericano de Defensa motivo del presente trabajo, es altamente valorado y elogiable por la disposición mostrada por las unidades y comandos especializados de Ciberdefensa y Ciberseguridad. El valioso material y experiencias permitirá ampliar el panorama para afirmar o reorientar el rumbo.

La Marina de México agradece la distinción de estar presente con esta aportación y les desea “buen viento y buena mar, para que puedan llevar la nave a puerto seguro”.

Buena práctica	Lección aprendida
• Análisis de Riesgos	• Fortalecer con metodologías de análisis estratégico: FODA, Coyuntural, Prospectivo, etc. • Planes para situaciones a corto, mediano y largo plazo.
• Planear antes de ejecutar. • Ciclo Deming (Planear Ejecutar Verificar Actuar).	• Resiliencia y adaptación durante la ejecución para lograr la evolución.
• Colaboración sector gobierno, privado y académico.	• Entre Fuerzas Armadas es posible. • El sector académico generó mayores beneficios
• Organización y división de responsabilidades.	• Organización por grupos de trabajo multidisciplinarios y colaborativos.
• Seguridad en capas o en profundidad.	• La seguridad en capas basada en el ser humano y la tecnología relacionada.
• Cooperación internacional.	• Mostrar disposición y cumplimiento.
• Normatividad.	• Promover los mecanismos para lograrla.

XI. Fuentes de consulta

https://www.gob.mx/semar

https://www.gob.mx/cms/uploads/attachment/file/457570/Ceremonia_de_Entrega-Recepci_n_de_la_Secretar_a_de_Marina_y_del_Mando_de_Armas_de_la_Armada_de_M_xico_1_Diciembre.pdf

https://www.gob.mx/semar/documentos/leyes-y-reglamentos-27612

https://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-082/17

https://www.gob.mx/cms/uploads/attachment/file/271884/Estrategia_Nacional_Ciberseguridad.pdf

https://www.gob.mx/cidge/documentos/infografias-del-maagticsi

https://www.gob.mx/semar/articulos/capitanias-de-puerto-a-la-secretaria-de-marina?idiom=es

https://www.gob.mx/universidadnaval

https://cesnav.uninav.edu.mx/cesnav/links_acc_progr/seginfor_site/seginfor_index.html

Coronel João Marinonio Enke Carneiro Ph.D. holds a Bachelor's Degree in Military Science from Agulhas Negras Military Academy (AMAN), a Master's Degree in Military Operations from Brazilian Army Captains Career School (EsAO) , Ph.D. in Military Sciences and Postdoctoral Research in National Defense from Brazilian Army Command and Staff College (ECEME). Colonel João Marinonio Enke Carneiro also has taken the Brazilian Army Strategy, Policy and Senior Management Course (CPEAEx) and a higher education certificate on Defense – Curso Superior de Defesa (CSD), from the Brazilian War College (ESG). At the Inter-American Defense College, he is in charge of developing and restructuring the Cyber Security Course..

BEST PRACTICES AND LESSONS LEARNED: CONCLUSIONS OF THE CONFERENCE

1. Introduction

As a professor of the Cyber Security / Public Security course at the Inter-American Defense College (IADC), I was privileged to organize the academic part of the Cyber Defense Conference at the IADC, which took place on November 5 and 6, 2019.

This Conference was conceived as a continuation of the 1st Western Hemisphere Cyber Defense Conference, promoted by the Inter-American Defense Board (IADB), which took place on May 14 and 15, 2019, in Bogotá, Colombia.

From the observations collected in Bogotá, we proposed the theme, Cyber Security and Defense - Best Practices and Lessons Learned. This topic was chosen due to the perceived need to promote the debate on better hemispheric cooperation in this area, which is absolutely vital for the advancement of the collective security effort for the countries of the Western Hemisphere.

This Conference met the IADB's objectives of: promoting the development of Cyber Defense policies and strategies in the Hemisphere, and strengthening cooperation mechanisms in Cyber Defense.

2. Why seek Best Practices and Lessons Learned?

In his book "Neorealism, States, and the Modern Mass Army"[1], Resende-Santos formulates what he called "Theory of Military Emulation". He justifies his theory by saying that "From the time humans began to organize themselves into political collectives, states have imitated

[1] Resende-Santos, João. Neorealism, States, and the Modern Mass Army, 2007. Cambridge University Press. ISBN-13 978-0-511-34293-6 Available at https://www.amazon.com/Neorealism-States-Modern-Mass-Army-ebook-dp-B0012K1OFC/dp/B0012K1OFC.

the best practices of one another: the latest in military weaponry, industrial processes, regulatory policy, even entire organs of state, such as central banks."

Resende-Santos also defines emulation as a voluntary, systematic and deliberate imitation by a state or any entity, which can update or modernize itself in a wide variety of areas, techniques, and practices of another state, customarily motivated or driven by competitive pressures. This can also occur within the framework of economic, administrative, regulatory and even constitutional practices.

He argues that innovating is costly and risky, time consuming and presents uncertain results. As competitiveness grows, states, in a careful assessment of potential risks and benefits, become more averse to risk, opting for the certainty of an immediate return from emulation, of which the results are known.

In turn, DiMaggio and Powell[2] introduce the concept of Isomorphism and its aspects, which are Mimetic Isomorphism, Coercive Isomorphism and Normative Isomorphism to the practice of emulation.

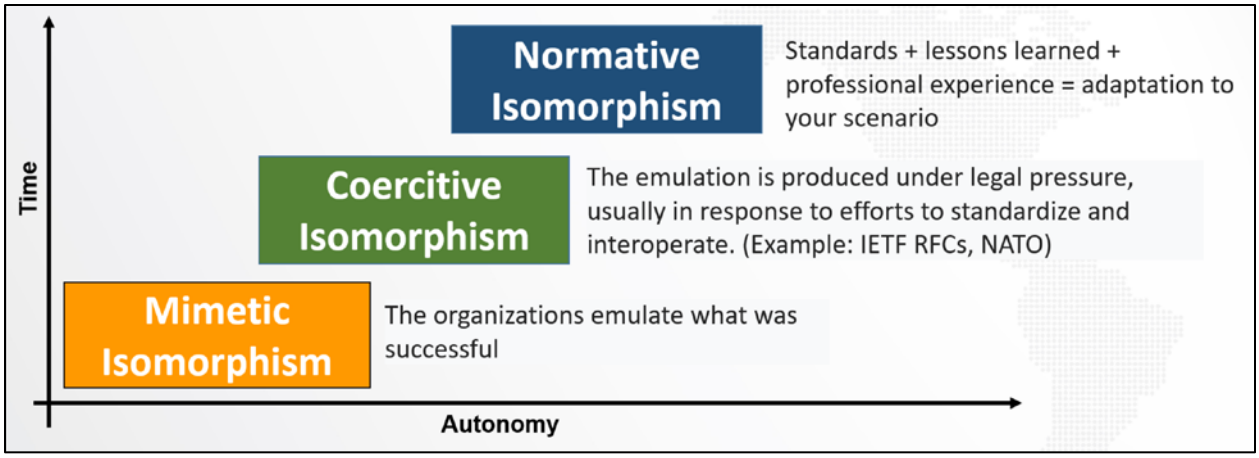
In Mimetic Isomorphism, organizations try to copy what was successful, without making significant considerations for adaptation or improvements. This is the way that can be implemented most quickly, but this lack of adaptation to reality significantly reduces the organization's autonomy.

In Coercive Isomorphism, the adoption of practices is conducted under legal pressure, usually in response to efforts for standardization and interoperability. Examples include the standardization of Internet protocols (RFCs - Request for Comments) made by the Internet Engineering Task Force (IETF) and NATO military doctrine.

In the most advanced form, the Normative Isomorphism, the standards are carefully compared with the lessons learned and the professional experiences of the organization's members. Through careful reflection, the rules are then adapted to reflect the reality of the organization's scenario, which takes more time but gives much greater autonomy.

In summary, we have:

[2] Powell, Walter et DiMaggio, Paul. *A Gaiola de Ferro Revisitada: Isomorfismo Institucional e Racionalidade Coletiva Nos Campos Organizacionais.* RAE Clássicos, vol 45, nº 2, p.74. Available at http://bibliotecadigital.fgv.br/ojs/index.php/rae/article/viewFile/37123/35894.



This Conference was very rich in content from the experiences presented by the participating countries. The majority contributed an article, or notes to compose this publication.

From the careful analysis of these contributions, we were able to extract nineteen (19) observations and conclusions below, which correspond to a summary of the ideas that were presented and discussed. For the more elaborate exposition of the concepts covered below, I suggest that you consult the articles and presentations made by the countries that participated in the Conference, that are also in this publication.

3. Observations and Conclusions

a. Use of program and project management methodologies

The implementation of the structures responsible for cyber-related actions in each country is a complex process, usually carried out within a Program or in a nation's Strategic Projects. To this end, the adoption of management methodologies for these Programs and Projects facilitates their conduct, reducing errors, carrying out better monitoring, and providing an adequate level of planning that allows a complex action to be carried out.

b. Clear and effective legal frameworks

One aspect addressed by almost all participants was the need to establish legal frameworks at the national level that support efforts related to Information Security, Cyber Security, and Cyber Defense. It is also essential to create legal authorities that support state agents in the actions necessary for their defense.

This effort has a broad spectrum and involves all levels, from policy-makers to technical elements that will conduct operations and keep networks secure. The speed that

characterizes the cyber sector represents a significant challenge for these frameworks to be produced and maintained at an adequate time so that they become effective.

c. Ability to work in a collaborative interagency environment

More than working within the services of the Armed Forces, it is essential to create a collaborative interagency environment, integrating efforts of the Armed Forces, Public Security, Justice, Government Agencies, those responsible for critical infrastructure, private sector, and the Academy. This attitude is not trivial, as it involves a wide variety of organizational cultures, different values, and sometimes conflicting interests.

d. Search for Consensus

Decisions that are the result of consensus are usually more effective and long-lasting than those that are imposed. The search for consensus, whenever possible, greatly facilitates the establishment of a collaborative environment.

e. Strengthening institutional relations with national and international actors

A collaborative environment needs to be established with national and international partners. The strengthening of institutional relations with these partners, integrating actions from the highest level, greatly facilitates activities at the lowest levels.

f. Proper planning horizon

The high speed of change imposed by technology modernization and the fluidity of the cyber domain limit long-term planning successes. Because of these factors, five years have proven to be a plausible strategic planning horizon for the cyber industry.

g. Establishing priorities and defining responsibilities

The large number of required actions combined with budget limitations require the establishment of priorities on what must be done first and who will be responsible for each action. The precise definition of priorities and responsibilities will significantly facilitate the management of Programs and Projects.

h. Perception of continuous processes

Authorities and organizations must realize that the Security and Cyber Defense of a state is a seemingly endless process that demand priorities of effort and adequate resources.

i. **Constant training**

Capacity building through courses and training, as well as participation in national or international exercises, should be continued, with talent identification being carried out as soon as possible.

j. **Training optimization**

Cyber training should be organized into specialty tracks, each with defined functions, and optimized into basic, intermediate, and advanced courses. If it is necessary to change the training path, this type of organization allows several courses to be reapplied, optimizing the track of the new training and saving financial resources and time.

k. **Structuring demand to obtain resources**

The resources will never be sufficient to carry out all the necessary cyber defense and security activities. When demand is structured, it becomes more evident to the decision-maker what should be prioritized and the amount of resources needed to carry out the chosen activities, allowing an effort to be funded accordingly.

l. **Incorporation in the country's political and strategic agenda**

Activities related to the cyber sector are strategic decisions for a country and need to discussed at the political level. This will allow priorization and resource allocation for the necessary defense of the state.

m. **Transversal effects of the cyber sector**

The cyber sector is transversal and has the potential to affect all society. Decision makers at all levels need to consider the scope of cyber threats.

n. **Sharing technical information in real-time**

Technical information related to cyber risks should be shared in real-time with national and international partners. An example of such an implementation is the automated indicator sharing (AIS) of the Cybersecurity and Infrastructure Agency (CISA), which shares cyber risk indicators between the US Federal Government and its national and international partners, including the private sector. Another platform that is already in use in the Hemisphere is the Malware Information Sharing Platform (MISP), which allows the exchange of information on the spread of malicious software, among others.

o. **Protection of critical infrastructures**

A country's critical infrastructure must be protected. As many of these infrastructures are owned or managed by the private sector, integration with these sectors becomes even more important.

p. **Supply chain protection**

The production of information technology equipment and network assets that are critical to a country must be verified and protected so that it does not suffer an interruption in its manufacture and supply.

q. **Implementation of cyber common security standards**

When ecosystem extensively implements common security standards, the possibility of exploitable flaws decreases significantly.

r. **Collective defense**

Cyber Defense needs to be seen as a collective security activity in the Hemisphere, taking advantage of the existing treaty framework and mutual assistance agreements between countries.

s. **Participation in international forums**

It was found that the most active international forum related to the cyber sector currently in the Hemisphere is the Ibero-American Forum for Cyber Defense. This forum was created in 2016 with the proposal to increase cooperation and integration of the digital security segments of the nations that make up the group. The current members are Argentina, Brazil, Chile, Colombia, Spain, Mexico, Paraguay, Peru, Portugal, and Uruguay. This forum annually promotes a conference and a cybernetic exercise integrating its elements. Participation in international forums like this facilitates the institutional and personal relationships of its members, improving the collaborative environment.

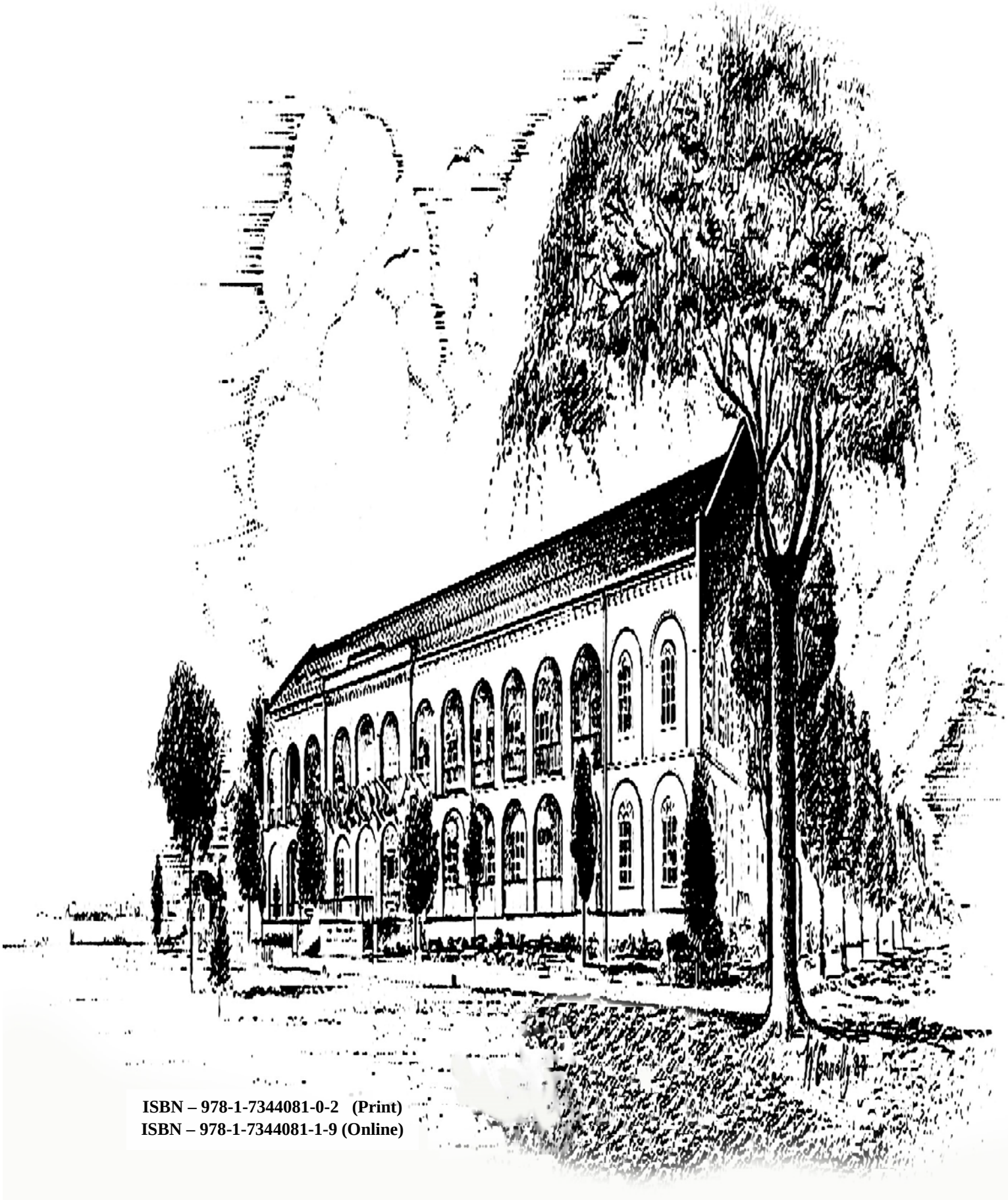
4. Next steps

The IADB is planning to hold a new Cyber Defense Conference in Lima, Peru on 14-15 Apr 2020. With this publication, we hope to inform the selection of the discussions topics, and contribute to increased knowledge of the cyber sector in the Hemisphere.

Una vez concluidos los dos días de presentaciones se solicitó a los ponentes que resumieran sus comentarios para esta publicación. El IADC no se hace responsable de las opiniones vertidas en los artículos publicados. Las opiniones, conclusiones y recomendaciones expresadas o que queden implicadas en sus distintos artículos son las de sus autores y no reflejan necesariamente la política o posición oficial ni del Colegio Interamericano de Defensa, ni de la Junta Interamericana de Defensa, ni de la Organización de Estados Americanas, ni la del país u organización representada por el autor.

Para más información, por favor, visite nuestra web www.iadc.edu.

Publicada en Washington, D.C. (EE.UU.). ISBN – 978-1-7344081-0-2 (Print); ISBN – 978-1-7344081-1-9 (Online).



ISBN – 978-1-7344081-0-2 (Print)
ISBN – 978-1-7344081-1-9 (Online)