CENTRE D'ÉTUDES
STRATÉGIQUES DE L'AFRIQUE
25 YEARS

Faire Progresser la Cybersécurité et la Stabilité Régionales en Afrique

Impact through Insight

PAIX, PROSPÉRITÉ ET
INTÉGRATION RÉGIONALE

Efforts et initiatives de l'IGAD en matière de cybersécurité

Atelier sur la promotion de la cyber-stabilité et de la cyber-sécurité régionales

21-23 mai 2024

Port Louis, Maurice

Nejat Abdulrahman Issa
SSP IGAD Senior PO

STRUCTURE

- Introduction - SSP IGAD, Vulnérabilité
- Efforts et initiatives
- Défis, réussites et leçons apprises

SSP IGAD

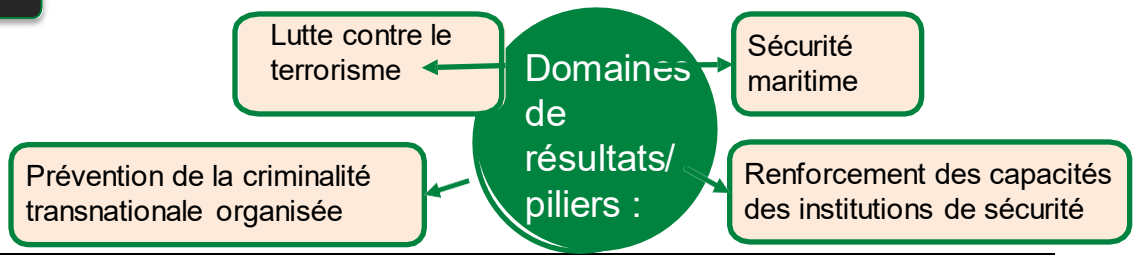
Pilier de la stratégie de sécurité et paix revitalisée de l'IGAD

Objectifs

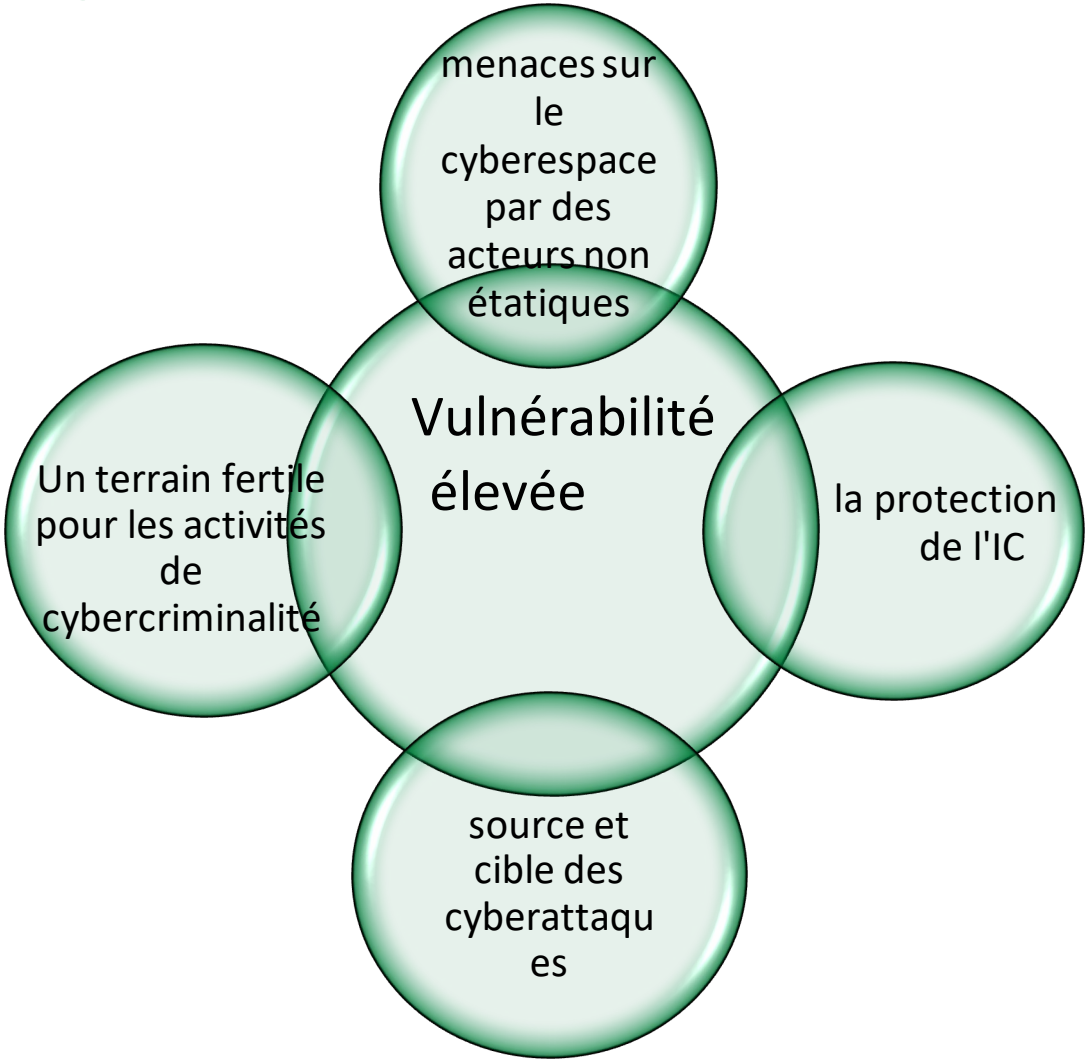
Renforcer les capacités institutionnelles et humaines de l'IGAD et de ses États membres en matière de prédiction, de prévention, de réaction et d'adaptation (PPRA) dans la lutte contre les EEE-TST (menaces transnationales émergentes, évolutives et existantes à la sécurité)

Domaines stratégiques prioritaires

- Renforcer la coopération et la coordination régionales
- Renforcement des capacités institutionnelles et humaines des États membres et de l'IGAD
- Amélioration des progrès en matière de ratification, d'intégration et de mise en œuvre des instruments régionaux et internationaux pertinents



Vulnérabilité



Efforts et initiatives

Renforcer la coopération et la coordination régionales

- À partir de 2013/4, étude, évaluation et consultation de divers praticiens des États membres en vue d'établir un mécanisme régional de coopération et de coordination par le biais de l'échange d'informations et de renseignements en matière pénale.

Renforcement des EM et de l'IGAD capacités institutionnelles et humaines

- Programmes thématiques de renforcement des capacités pour la sensibilisation, l'acquisition de compétences et de connaissances, la création de réseaux informels et le renforcement de la confiance en soi :
  - Techniques d'enquête sur la cybercriminalité
  - Rôle de la technologie et des plates-formes en ligne, des SM en tant qu'outils de recrutement
  - Cyber/expertise numérique/preuves sur la Lutte contre la traite des personnes (CTIP)
  - Examen des cadres de cybersécurité des EM
  - Menaces à la sécurité des drones et des technologies émergentes

Amélioration des progrès en matière de ratification, d'intégration et de mise en œuvre des instruments pertinents

- Sensibilisation et promotion des instruments juridiques disponibles, y compris les lacunes identifiées, les défis et les réussites.

Projets suivants

- Poursuite des programmes de renforcement des capacités, promotion des instruments juridiques
- Évaluation approfondie des cadres de cybersécurité existants, de leurs capacités et de leurs limites
- Élaboration d'une stratégie régionale en matière de cybersécurité

IGAD
SSP
Security Sector Programme

Défis

États membres

- Protection des données personnelles (PDP) — d'énormes quantités de données personnelles sont collectées, stockées et transmises dans le monde entier
- Souveraineté numérique
- Confiance entre le gouvernement et la communauté
- les transformations numériques et l'utilisation de la technologie au sein des prestataires de services publics — Internet, réseaux mobiles et outils TIC connexes

Institutionnel — LEA

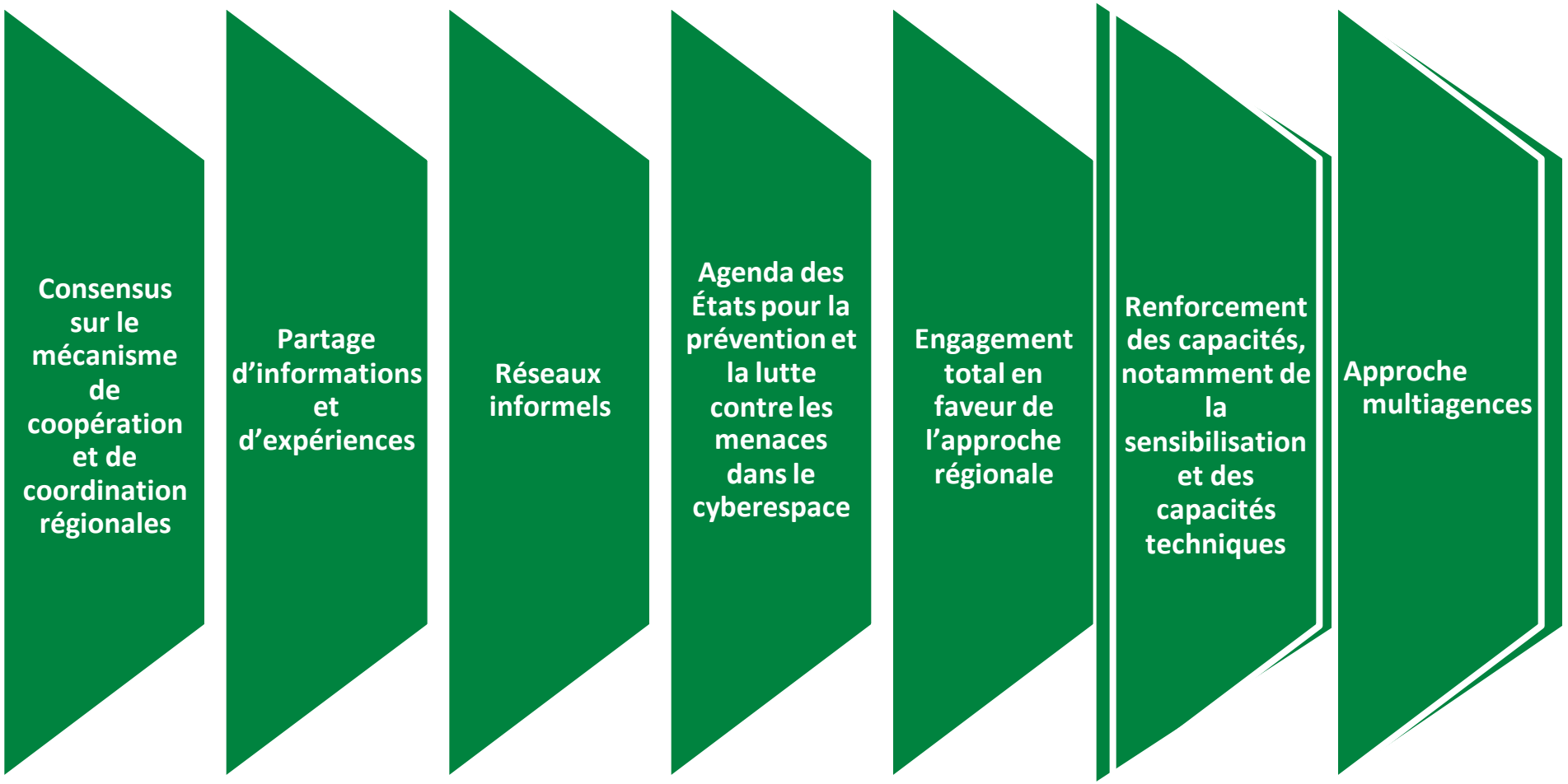
- Faible capacité/capacité technique
- sensibilisation, capacité de détection, d'enquête, d'acquisition de données médico-légales, de poursuites, questions de ressources humaines - comment équilibrer et utiliser, etc.
- Ressources et progrès technologiques — nouvelles technologies, infrastructures, accessibilité, etc.
- Faiblesse de la législation et de sa mise en œuvre
- Absence d'informations complètes sur les réseaux transnationaux opérant dans le cyberespace

Régionale

- Différents niveaux de menace pour les EM — affectant la priorité et la réponse
- pratique des engagements bilatéraux

IGAD
SSP
Security Sector Programme

Succès et leçons apprises



IGAD
SSP
Security Sector Programme

Merci pour votre attention !

Nejat Abdulrahman Issa
Chargé de programme principal **IGAD SSP**

Nejat.Abdulrahman@igad.int

@NejatIssa @IGADISSP

SSP
Security Sector Programme

CENTRE D'ÉTUDES
STRATÉGIQUES DE L'AFRIQUE

25 YEARS

Faire Progresser la Cybersécurité et la Stabilité Régionales en Afrique

Impact through Insight

Vue d'ensemble du cadre de cybersécurité de la CDAA

Présenté à : Atelier sur l'avancement de la stabilité et de la sécurité cybernétiques régionales

Présenté par : Dr. George Ah-Thew, SPO TIC de la CDAA

22 mai 2024

Port Louis, Maurice

U.S. DEPARTMENT of STATE

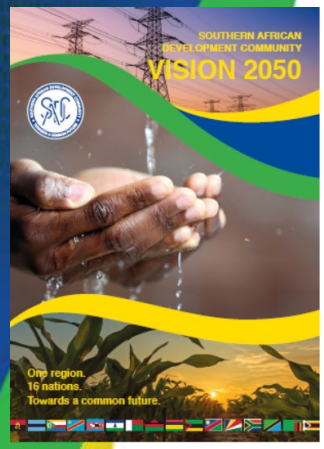
AFRICA CENTER FOR STRATEGIC STUDIES

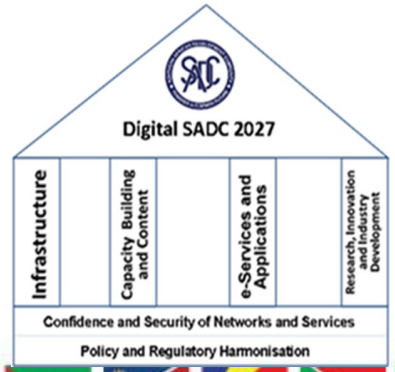
Schéma de présentation

- Contexte
- Cadre et mise en œuvre juridiques et réglementaires harmonisés de la CDAA en matière de cybersécurité
- Réalisations, défis et leçons apprises
- Recommandations

Contexte

- La CDAA comprend 16 États membres et une population estimée à 360 millions de personnes.
- La **Vision 2050 de la CDAA** repose sur la paix, la sécurité et la bonne gouvernance et s'appuie sur trois piliers, qui sont liés entre eux et dont les questions transversales sont l'égalité des sexes, la jeunesse, l'environnement et le changement climatique, ainsi que la gestion des risques de catastrophe. **Pilier II** : Développement des infrastructures à l'appui de l'intégration régionale.
- **Digital CDAA 2027** est le chapitre TIC du **plan directeur de développement des infrastructures régionales** de la CDAA (RIDMP) 2012-2027, le plan directeur pour le développement des infrastructures TIC dans la région de la CDAA. Le RIDMP s'appuie sur le principe « Garantir la **confiance et la sécurité des réseaux et des services** ».



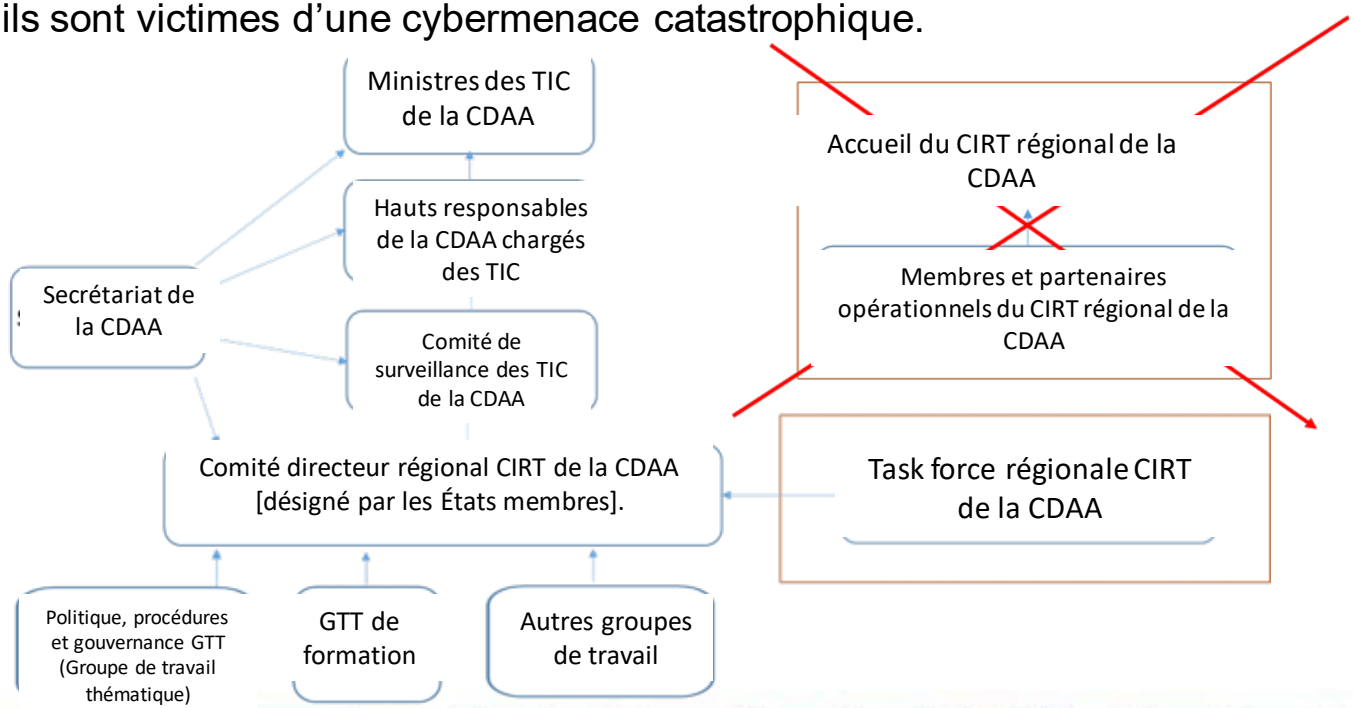


Cadre et mise en œuvre juridiques et réglementaires harmonisés de la CDAA en matière de cybersécurité

- Le cadre juridique et réglementaire harmonisé de la CDAA en matière de cybersécurité se compose de trois (3) lois types sur la cybersécurité élaborées dans le cadre du projet HIPSSA et approuvées en novembre 2012 :
  - Loi type de la CDAA sur le commerce électronique et les transactions ;
  - **Loi type de la CDAA sur la protection des données ;** et
  - **Loi type de la CDAA sur la cybercriminalité**.
- Tous les États membres ont transposé les lois types de la CDAA sur le commerce électronique, les transactions électroniques et la cybercriminalité ou disposent d'un cadre juridique existant. Treize (13) États membres ont mis en place des lois sur la protection des données.
- Les lois types de la CDAA sur la protection des données et la cybercriminalité ont été révisées. Ils comprennent chacun, des lignes directrices de mise en œuvre et un calendrier et sont en cours d'adoption par les États membres.
- Cinq (5) États membres ont ratifié la Convention de l'UA sur la cybersécurité et la protection des données personnelles (Convention de Malabo) de 2014 qui est entrée en vigueur le 8 juin 2023.

Cadre et mise en œuvre juridiques et réglementaires harmonisés de la CDAA en matière de cybersécurité

- Neuf (9) États membres ont mis en place leur CIRT national.
- Les exercices annuels de cybernétique de la CDAA continuent de renforcer les capacités des agents CIRT, y compris des postes et des banques centrales.)
- Mise en place du **cadre régional CIRT de la CDAA (SR-CIRT)** en septembre 2019 — Une plate-forme de collaboration régionale pour le renforcement des capacités régionales de préparation, de protection et de réponse aux incidents en matière de cybersécurité.
- L'hôte de la SR-CIRT a été rendu opérationnel par la création de la task force SR-CIRT, qui compte actuellement 8 membres (chefs des CIRT) chargés d'aider les États membres s'ils sont victimes d'une cybermenace catastrophique.



Réalisations, défis et leçons apprises

- Les États membres se situent à des niveaux de développement différents et certains ont besoin d'aide pour transposer les lois types révisées de la CDAA.
- La cybersécurité est une responsabilité partagée et chacun a un rôle à jouer, ce qui nécessite une action coordonnée.
- Le cadre juridique et réglementaire de la cybersécurité nécessite des mécanismes institutionnels d'application (par exemple, CIRT/LPD) que certains États membres doivent encore mettre en place.
- Les États membres leaders jouent un rôle de premier plan et soutiennent ceux qui sont à la traîne (par exemple, l'échange entre pairs/le parrainage des membres du « FIRST »).
- Initiatives cohérentes et inclusives de renforcement des capacités (par exemple, entraînements en cybernétique) en matière de TTX dans les domaines identifiés par les États membres (par exemple, industrie postale/financière).
- L'Académie de cybersécurité de Maurice (CERT-MU) soutient la CDAA et l'Afrique en proposant des cours gratuits de cybersécurité via la « ITU Academy ».
- Le soutien de l'IUT (élaboration de lois types et cyber entraînement) et des institutions continentales (par exemple AfricaCERT), des partenaires de coopération internationale (PIC) et des organismes de mise en œuvre des TIC de la CDAA (par exemple ARCA/SATA) a eu un impact significatif.

Recommandations

- Mécanisme d'assistance technique (« TA ») pour aider les États membres qui en ont besoin à transposer dans leur droit interne les lois types révisées de la CDAA sur la protection des données et la cybercriminalité, ce qui permettra d'harmoniser les législations dans l'ensemble de la CDAA.
- Soutenir les États membres dans la mise en place de leur CIRT/LPD et l'opérationnalisation du CIRT régional de la CDAA (SR-CIRT), ainsi que les liens avec d'autres CIRT/partenaires régionaux.
- Soutenir la ARCA dans la mise en place de la LPD régionale de la CDAA.
- Soutenir l'élaboration de la stratégie de cybersécurité de la CDAA, qui comprendra une analyse de la situation et une évaluation de la maturité cybernétique.
- Renforcer l'académie de cybersécurité existante (par exemple, le CERT-MU) et soutenir le centre d'excellence régional de la CDAA en matière de technologies de l'information et de la communication.
- Éviter les doubles emplois et soutenir les initiatives de cybersécurité pilotées par les CER et menées par les chefs de la région.
- Offrir des bourses par l'intermédiaire des CER et un accès gratuit à des possibilités de formation spécialisée afin de renforcer le vivier d'experts régionaux en cybersécurité.
- Organiser un forum continental sur la cybersécurité, afin d'attirer également les jeunes.
- Créer un laboratoire de la CDAA sur les preuves numériques et la cybercriminalité — Identification, saisie, acquisition, examen et maximisation de la valeur des preuves électroniques.

CENTRE D'ÉTUDES
STRATÉGIQUES DE L'AFRIQUE
25 YEARS

Faire Progresser la Cybersécurité et la Stabilité Régionales en Afrique

Impact through Insight