3 DÉCEMBRE 2024

Euro Space Center - Galaxia – Transinne

Dossier de presse

IDELUX et Cyberwal by Digital Wallonia sont heureux de vous convier à leur conférence de presse pour découvrir les enjeux et les innovations qui marqueront la troisième édition de l'École "Cyberwal in Galaxia Program" !

La Wallonie démontre une nouvelle fois son rôle prépondérant dans le développement de solutions de cybersécurité au niveau mondial.

L'École européenne Cyberwal a ouvert ses portes pour cette troisième promotion, réunissant une nouvelle fois plus de 200 étudiants internationaux, du 2 au 6 décembre, à l'Euro Space Center de Transinne.

TABLE DES MATIÈRES

Contexte mondial

En 2024, l**es défis liés à la cybersécurité ont atteint une complexité et une urgence sans précédent**. Les entreprises, gouvernements et individus sont continuellement menacés par des cybercriminels de plus en plus habiles et innovants. Les enjeux s'étendent à plusieurs domaines clés, notamment la **protection des infrastructures critiques** qui sont vitales pour le fonctionnement de la société, ainsi que la gestion de la vie privée et la **sécurité des données** personnelles.
L'évolution rapide des technologies, en particulier avec l'adoption massive de l'**Internet des Objets** (IoT) et l'intégration croissante de l'**intelligence artificielle** dans les processus quotidiens, exacerbe ces défis.

Coût astronomique de la cybercriminalité

Le coût de la cybercriminalité au niveau mondial est en **constante augmentation.** Selon un rapport de Cybersecurity Ventures, le coût annuel de la cybercriminalité devrait atteindre environ **10,5 billions de dollars d'ici 2025**, contre 3 billions de dollars en 2015. Cette projection fait de la cybercriminalité l'**une des menaces économiques les plus graves de notre époque.**

Ce coût englobe **plusieurs aspects qui affectent les entreprises à différents niveaux**. Tout d'abord, les pertes directes incluent non seulement l'**argent volé** par les cybercriminels mais aussi les fonds souvent conséquents payés en rançon lors des attaques de ransomware. Ensuite, le **coût de la récupération** peut s'avérer également très important. Après une attaque, les entreprises sont contraintes d'investir massivement pour restaurer les données et les systèmes affectés, ce qui implique des dépenses en matériel et logiciel, ainsi que les services de professionnels pour la restauration des données et la sécurisation des systèmes.

Les **pertes de productivité** sont une autre conséquence majeure des cyberattaques. Ces dernières peuvent complètement paralyser les opérations d'une entreprise, résultant en des pertes de productivité significatives qui peuvent avoir un impact prolongé sur le fonctionnement de l'entreprise. De plus, la **réputation et la confiance des clients** sont souvent sévèrement touchées par une attaque réussie, entraînant une perte de clients actuels et potentiels, et un impact négatif sur la fidélité à long terme des consommateurs et partenaires commerciaux.

En outre, les entreprises qui subissent des violations de données peuvent être confrontées à **des amendes et des sanctions réglementaires**, particulièrement si elles ne sont pas conformes à des réglementations strictes telles que le RGPD en Europe. Ces amendes peuvent être conséquentes et ajouter un fardeau financier supplémentaire aux coûts déjà engendrés par l'attaque elle-même.

Enfin, avec la **montée des cyberattaques**, les primes d'assurance cybernétique ont également augmenté, devenant un poste de coût pour les entreprises qui cherchent à se couvrir contre les risques de cybersécurité.

Ces divers aspects soulignent la nécessité impérieuse pour les entreprises de toutes tailles d'**investir dans des mesures de cybersécurité robustes** et de **former continuellement** leurs employés pour se défendre contre ces menaces croissantes.
La révolution numérique impose donc aux organisations de tous secteurs d'adapter leurs **stratégies de sécurité** pour contrer des menaces toujours plus sophistiquées, telles que le phishing, les ransomwares, les attaques sur la chaîne d'approvisionnement ou encore les intrusions dans les réseaux.

Croissance exponentielle du marché de la cybersécurité

Le marché de la cybersécurité connaît une **croissance exponentielle,** stimulée par la nécessité impérieuse de protéger les infrastructures et les données critiques. Les investissements dans des solutions de sécurité avancées et les formations spécialisées en cybersécurité sont devenus des **priorités stratégiques** pour toutes les structures, grandes comme petites, qui cherchent à diminuer drastiquement les risques et à se conformer aux réglementations de plus en plus strictes en matière de protection des données.

Renforcer la sécurité collective

En outre, la coopération entre les organisations de toutes tailles est essentielle pour **renforcer la sécurité collective.** Les **échanges d'informations** sur les menaces, les pratiques de sécurité recommandées et les **initiatives de formation** peuvent aider à élever le niveau de préparation et de résilience de l'ensemble du tissu économique. Ainsi, les gouvernements et les institutions réglementaires jouent également un rôle fondamental en établissant des normes et des directives claires pour la cybersécurité, aidant ainsi les entreprises à naviguer dans le paysage complexe des menaces numériques et à mettre en œuvre des pratiques de sécurité robustes.

Tendances actuelles et défis associés à la cybersécurité :

- **Croissance du marché de la cybersécurité** : en 2023, le marché mondial de la cybersécurité a atteint **environ 200 milliards de dollars**, une progression significative qui reflète l'urgence croissante des besoins en sécurité informatique. Cette croissance est stimulée par la numérisation accélérée des entreprises et l'augmentation des cyberattaques, ce qui pousse les entreprises à investir davantage dans des solutions de cybersécurité solides.

- **Diversification des menaces** : les attaques deviennent de plus en plus sophistiquées, allant des ransomwares aux attaques de phishing, en passant par les violations de données et les attaques contre l'infrastructure cloud. Cette diversité de menaces nécessite des **réponses tout aussi diversifiées et spécialisées**, poussant les entreprises à adopter des stratégies de sécurité multicouches.

- **Ciblage des PME**: il est généralement reconnu que les PME, étant particulièrement vulnérables aux cyberattaques en raison de ressources limitées et souvent d'une moindre **sensibilisation aux risques**, sont un secteur en croissance rapide pour les solutions de cybersécurité. Les fournisseurs de ces solutions ciblent de plus en plus les PME avec des produits adaptés à leurs besoins et budgets spécifiques, facilitant ainsi leur adoption.

- **Défis liés à la pénurie de compétences** : malgré la croissance du marché, le secteur de la cybersécurité fait face à une pénurie significative de compétences spécialisées. Les entreprises peinent à recruter des professionnels qualifiés, **ce qui entrave leur capacité à mettre en œuvre des mesures de sécurité efficaces**. Cette pénurie appelle à des stratégies innovantes en matière de formation et de développement des compétences.

- **Investissements et innovations technologiques** : l'innovation technologique est essentielle **pour rester à la pointe de la défense contre les cybermenaces.** Les entreprises investissent dans des technologies avancées telles que l'intelligence artificielle pour automatiser la détection des menaces et la réponse aux incidents, ce qui permet une réactivité plus rapide et plus efficace.

- **Impact réglementaire et conformité** : la régulation joue un rôle de plus en plus central dans le domaine de la cybersécurité. Avec des réglementations comme le RGPD en Europe, les entreprises doivent non seulement protéger leurs réseaux mais aussi **garantir la conformité avec les législations en vigueur,** ce qui ajoute une couche de complexité à la gestion de la sécurité.

La souveraineté européenne

La montée rapide et soutenue des **cybermenaces** rend essentiels **l'engagement et la sensibilisation** des gouvernements, des institutions, des acteurs économiques et de la société civile aux risques associés à la cybercriminalité. Face à ces défis, **l'Europe** a placé le développement de solutions de cybersécurité avancées et flexibles au sommet de ses priorités.

Les instances telles que le **Conseil européen** et la **Commission européenne**, conscientes de cette nécessité absolue, ont intensifié leurs investissements dans la recherche, l'innovation et la formation pour garantir la sécurité numérique de nos sociétés.

Georges Cottin, Conseiller général de l'intercommunale IDELUX, souligne l'ambition claire de cet effort : **propulser la Wallonie,** et par extension l'Europe, au rang de **leader en matière de cybersécurité,** faisant du continent un modèle de résilience cybernétique.

Chiffres clés du marché de la cybersécurité en Europe

1. La valeur du marché est projetée à atteindre **environ 105,17 milliards d'euros d'ici 2029.**
2. Le taux de croissance annuel composé (CAGR) pour les services de cybersécurité gérés est prévu **à 11,5 % entre 2024 et 2030.**
3. Le segment des déploiements basés sur le cloud devrait croître à un CAGR **de 12,9 % de 2024 à 2030.**
4. Les petites et moyennes entreprises connaîtront **la croissance la plus rapide** en matière d'adoption de la cybersécurité.
5. En 2024, le marché est prévu de générer **environ 43,41 milliards d'euros de revenus**, avec **environ 23,41 milliards d'euros provenant des services de sécurité.**

En Belgique

La cybersécurité est une **priorité nationale**, reflétant l'importance croissante des technologies numériques dans tous les secteurs d'activités ainsi que la présence de nombreuses institutions européennes et internationales. Le pays reconnaît que les infrastructures numériques sont essentielles à la stabilité économique et à la sécurité nationale, surtout **dans un contexte où Bruxelles est qualifié de "capitale de l'Europe"**. Cette centralité renforce la nécessité de protéger les réseaux contre les cyberattaques qui pourraient compromettre des informations cruciales à l'échelle notamment de l'Union européenne.

Développement à Transinne d'un pôle d’excellence en cybersécurité

Pour répondre à ces défis, la Wallonie s’est dotée d’une **stratégie globale**.

- **L’école Cyberwal in Galaxia Program**

Pour répondre aux défis croissants de la cybercriminalité, la Wallonie a élaboré une politique stratégique de cybersécurité nommée **« Cyberwal by Digital Wallonia »**. Cette initiative vise à protéger non seulement le territoire mais également les divers acteurs sociaux et économiques présents.

Intégrée dans le **Plan de relance wallon (PRW)**, Cyberwal a bénéficié de **financements conséquents** en 2022, 2023 et 2024 permettant de lancer ou d'étendre des programmes structurants tels que des écoles de recherche et la mise en place de démonstrateurs, notamment le projet CyberExcellence. Ces efforts visent à unifier les acteurs de la cybersécurité en Wallonie — des universités aux centres de recherche en passant par les entreprises innovantes — autour d'un pôle d'excellence. Ce pôle ambitionne de créer un environnement favorable au développement d’un écosystème robuste dédié à la cybersécurité.

Dans ce contexte dynamique, **la troisième édition** de l'école internationale Cyberwal, qui se déroule actuellement à l'Euro Space Center de Transinne, du 2 au 6 décembre, **affiche complet** chaque jour avec une capacité maximale de 150 personnes. Cette année, ce sont plus de **200 étudiants européens** qui participent, démontrant une croissance significative par rapport aux deux éditions précédentes (140% de participants en plus par rapport à l’édition 2022 et un pourcentage d'augmentation du nombre de participants par jour de près de 90% par rapport à l’édition 2023).

Photo de l’édition 2024

Programme

Day 1
Monday 02/12

AI and Cybersecurity day 2024

The rise of artificial intelligence (AI) is having a profound impact on our society. During 2024, AI continues to be rapidly integrated into various sectors, each leveraging the technology to **improve efficiency, reduce costs, and provide better services**. The use of AI has expanded across industries, but some sectors have seen particularly high levels of adoption and integration such as **healthcare** (diagnostics, drug discovery, personalized medicine, predictive analytics), **finance** and **banking** (fraud detection, algorithmic trading, credit scoring, customer service), **retail and e-commerce** (personalized recommendations, inventory Management, customer service, pricing optimization), **manufacturing and industry 4.0** (predictive maintenance, quality control, supply chain optimization, robotics and automation), **automotive and transportation** (autonomous vehicles, driver assistance systems, logistics and fleet management, predictive maintenance), **energy and utilities** (Smart Grid management, predictive maintenance, energy consumption optimization, renewable energy management), telecommunications (network optimization, predictive maintenance, customer support, fraud detection) and **education** (personalized learning, automated Grading, tutoring systems, administrative efficiency). AI is having impact and driving innovation by providing improved efficiency, increased productivity, better decision-making, improved healthcare, or environmental sustainability.

AI research has advanced in 2024 with **advancements in Large Language Models** (more powerful models, fine-tuning and adaptability, reduced hallucinations), generative AI and multimodal models (image and text integration, video and audio generation, creative applications).

However as AI and machine learning systems become more prevalent and integral to various applications, they also become **more attractive targets for cyberattacks**. Some of the new and evolving cybersecurity threats to AI and machine learning in 2024 are adversarial attacks, data poisoning, model inference attacks, model evasion attacks, backdoors attacks, membership inference attacks, federated learning Attacks, supply chain attacks and cloud infrastructure attacks. **Cybersecurity is important for AI** because AI systems are increasingly being used in critical infrastructure, such as power grids and transportation systems. If these systems are hacked, it could have a devastating impact on society.

The objective of the day is to **present some key research topics at the intersection of AI and cybersecurity in the form of short tutorials or research presentations**. The day will address topics on how AI is being used for threat identification, protection, detection, response and recovery. More specific topics such as Explainable AI for malware analysis, AI based AI-powered anomaly detection, AI-powered malware detection and AI-powered incident response will also be addressed.

09:00 AM - 10:00 AM
REGISTRATIONS

10:00 AM - 10:05 AM | Auditorium
Introduction
Philippe Massonet - Scientific Coordinator at CETIC

10:05 AM - 11:00 AM | Auditorium
Statistical Model Checking for Secure Cyber-Physical Systems

Cyber-physical or ***IoT systems*** are ubiquitous in modern society, and involve computational devices monitoring and controlling complex physical systems. The computational devices are often constrained by computational power, memory, and energy consumption, and are increasingly used ***in critical industrial systems***. Clearly the ***safety and security*** of such systems is of the utmost importance. In this talk we will present a number of settings, where ***so-called Statistical Model Checking (SMC)*** -- supported by the award-winning tool ***UPPAAL*** (www.uppaal.org) – has been used to identify and quantify potentially security side-channel attacks.

In order to formally ***specify security-related properties***—such as non-interference—one cannot purely rely on traditional trace-based specification formalisms such as ***Linear Temporal Logic*** (LTL). The reason is that they relate the events of two (or more) traces of the system, and LTL can only reason on one execution at a time. So-***called hyper-property extensions*** of LTL has been proposed. Within UPPAAL a ***real-time and probabilistic hyper-logic (HPSLT)*** has been implemented and used to identify three types of side-channel attacks.

DTLS is a protocol that is widely used by ***IoT devices***, including critical industrial IoT systems, as the transport layer for secure and authenticated communication. A formal model of DTLS has been made, and the statistical model checking engine of UPPAAL has been used to analyse, evaluate, and optimise ***energy consumption for the protocol***. In particular different network scenarios has been considered identifying how energy consumption is highly dependent on the specific usage scenario. Addressing security issues the model has been extended with an ***active attacker*** trying to drain as much energy as possible from the target system by (ab)using DTLS. Analysing and preventing such ***Denial of Service attacks*** is essential for critical systems.

Finally, we will report on use of the statistical model checking engine of UPPAAL for analysing ***impact of bit-flips*** in security critical code.

AI has revolutionized cybersecurity, enabling advanced capabilities such as the detection of malware, vulnerabilities and fraud. Yet, as AI empowers defenders, it also empowers attackers. The dark side of AI reveals a landscape where malicious actors harness AI for spear phishing, automated cyberattacks, misinformation, and deepfakes. Moreover, AI itself becomes a target, as shown by adversarial machine learning and model poisoning attacks. Finally, there are concerns about AI creating a dystopia.

The talk further delves into novel technologies such as attribution (watermarking) and computing on encrypted data that can play a role in mitigating some of these risks.

Overall, there is a need for a multidisciplinary approach encompassing technology, regulation, and ethics to effectively address the challenges presented by the intricate relationship between AI, cybersecurity and privacy.

Kim Guldstrand Larsen - Professor at Aalborg University, Department of Computer Science, Denmark

11:00 AM – 11:45 AM | Auditorium
Machine Learning Security in the Real World

Adversarial attacks are considered as one of the most critical security threats for Machine Learning (ML). In order to enable ***the secure deployment of ML models*** in the real world, it is essential to properly assess their robustness to adversarial attacks and develop means to make models more robust. Traditional adversarial attacks were mostly designed for image recognition and assume that every image pixel can be modified independently to its full range of values.

In many domains, however, these attacks fail to consider that only specific perturbations could occur in practice due to ***the hard domain constraints*** that delimit the set of valid inputs. Because of this, they almost-always produce examples that are not feasible (i.e. could not exist in the real world). As a result, research has developed ***real-world adversarial attacks*** that either manipulate real objects through a series of problem-space transformations (i.e. problem-space attacks) or generate feature perturbations that satisfy predefined domain constraints (i.e. constrained feature space attacks). In this talk, we will review the scientific literature on these attacks and report on our experience in applying them to real-world cases.

Maxime Cordy - Research Scientist at the Interdisciplinary Center for Security, Reliability and Trust (SnT)

11:45 AM – 12:00 PM
COFFEE BREAK

12:00 PM – 01:00 PM | Auditorium

Turing's Echo on Deceptive Machines: The Challenge of Distinguishing Human and AI Creations

As generative AI models evolve, distinguishing between human-generated and AI-generated content is becoming increasingly challenging, threatening trust across various domains such as misinformation in media, political campaigns, legal accountability, scientific integrity, and cybersecurity. Distinguishing between machine and human outputs will be vital because, in the dystopian future, machines will potentially rise against humans.

This talk explores methods and technologies for identifying the origin of content, focusing on audio and text. We highlight the limitations of current models in detecting subtle differences between human-generated and AI-generated content. Our work augments physical principles, such as the Micro Doppler Effect, with machine learning frameworks. This integration incorporates prior input data knowledge into the model, enhancing detection and reducing biases in generated content. Finally, we discuss ongoing challenges and future research directions in this dynamic field.

Ahmad-Reza Sadeghi - Professor Dr.-Ing. at technische universität darmstadt

01:00 PM – 02:00 PM
LUNCH TIME

02:00 PM – 03:30 PM | Auditorium

Explainable ML for malware analysis

The talk addresses the growing complexity of ***malware*** by exploring advanced detection and analysis techniques, focusing on both ***static*** and ***dynamic*** approaches. The lecture highlights the strengths and limitations of each approach and discusses their combination to improve detection accuracy. A method of r***epresenting malware as images*** is introduced, allowing the application of image processing and machine learning techniques to detect malicious patterns, offering advantages over traditional methods. The importance of ***explainability*** in malware detection is advocated by using such approaches.

Fabio Martinelli - Research Director at National Research Council of Italy

03:30 PM – 03:45 PM
COFFEE BREAK

03:45 PM – 04:30 PM | Auditorium

Cybersecurity threat landscape, Microsoft's view on the current and future secure state

During this session, Microsoft will show their view on the ***threat landscape*** and how is has evolved throughout the years using ***geopolitical*** challenges, technical advancements by integrating ***cutting-edge technologies*** into their attacks and how we should
prepare, defend and collaborate as one to become more resilient and secure in this ever-changing world

Bart Asnot - National Security Officer at Microsoft

04:30 PM – 05:15 PM | Auditorium

Artificial Intelligence Deployable Agent (AIDA)

Contemporary combat systems carry an increasing amount of ***tactical computing*** and electronics potentially vulnerable to ***cyber-attacks***. While current cyber-defense operations address in non-real time the needs for detection and response to cyber incidents affecting traditional IT systems, securing the fast expanding Internet of ***Military Things*** (IoMT) requires ***very short response times***, and accurate decision making under *strong* **operational, computing and energy constraints**. *The* deployment of efficient detection and response capacities on embedded systems requires the design of lightweight resident **Artificial Intelligence (AI) agents**, *trained specifically for* these environments and capable of automating the detection and response loop in the absence of timely available ***human expertise***. NATO's IST-152 Research Task Group (2016-2020) on "Intelligent, Autonomous and Trusted Agents for Cyber Defense and Resilience" (AICA) initiated this concept between 2016 and 2020. The research yielded an ***AICA Reference Architecture*** (Kott et al., 2018). Later, an international working group formed to continue work on AICA (see https://www.aica-iwg.org/).

Yet this highly conceptual architecture was not yet set into practice. The growing use of ***Unmanned Vehicles (UxV)*** in modern conflicts however revives the need for time sensitive autonomous decision at the edge of systems evolving in environments saturated with ***Cyber-Electromagnetic Threats*** (CEMA). To reduce UxVs exposure and augment their chances of survival in contested battlefield, remote control is progressively replaced by individual (***autonomous***) and collective (***swarm***) intelligent navigation techniques. While AI is seen as an essential capability for the survival of these proliferating objects, ***adversarial AI*** discipline unveils targeted evasion techniques to lure and hide from embedded AI. In short we need cyber-defense agents that are altogether ***frugal, accurate, adaptive, explainable, collaborative, and robust***. This is the challenge addressed by AIDA project. The proposed solution relies on three types of AI agents: a ***white agent***, a ***red agent***, and a ***blue agent***. The white agent is a ***foundation model*** that is trained against massive data to develop a broad set of ***human-like capacities*** such as threat analysis, detection rule edition, incident qualification and response planning. Cyber-defense analysts prompt a ***Large Language Model*** (LLM) upon identification of new threats to produce tailored ***detection rules*** and ***response plans*** in seconds instead of hours. A ***Retrieval Augmented Generation (RAG)*** procedure restricts LLM sources to qualified knowledge bases.

A ***reward system*** based on ***human feedback*** reinforces the model toward good decisions. From this white agent, smaller, more ***specialized agents*** will be derived that aim to perform narrow cyber-defense routines ***at the edge of IoMT***. Unlike the white agent, ***blue agents*** need to operate in resource-constrained environment in an ***autonomous*** manner. We will use pruning and unlearning techniques to minimize the resource requirements of blue agents and obfuscation techniques to reduce their exposure to reverse engineering. Wherever needed, they will be ***fine-tuned*** to their environment of destination across ***land, sea, air, space and cyber*** domains. Yet as we may lack quantitative attack data, we will craft a third type of agent, whose role will be to ***generate attacks***. The ***red agent*** will be trained in a simulated environment placed in adversarial setup with blue agents to develop offensive AI strategies. This ***Generative Adversarial Networks (GAN)*** setup will reinforce blue agents' successful defense strategies, challenge their individual and collaborative defense objectives, and strengthen their ***robustness*** towards evasion attacks.

To conclude, the AIDA system involves an ***LLM (white agent)***, *adversarial* **generative AI (red agent)** *and a* **Multi-Agent System (blue agents)** *in mission-critical activities landing in 5 military domains. Among other applications, the system aims to protect combat aircraft against* **CEMA threats** *with severe safety implications. Continuous improvement and responsible use of AI are enabled by* **reinforcement** *learning and* **RAG** *techniques. It reduces the exposure of modern military systems to emerging risks such as adversarial AI attacks.AI are enabled by reinforcement learning and RAG techniques. It reduces the exposure of modern military systems to emerging risks such as* **adversarial AI attacks**.

Adrien Becue - AI & Cybersecurity Expert at THALES

05:15 PM – 05:30 PM | Auditorium

Kick-off SecuWeb: Towards a new and safer internet

SecuWeb aims to strengthen data security in companies and organisations in Flanders, Wallonia and France. The project investigates how innovative technologies such as Solid, Blockchain, Quantum Internet, 5G, AI and IoT can contribute to safer data use. Through demonstrators and use cases, we explore how to implement these technologies in companies and organisations. We focus on key sectors for our regions such as healthcare, industry 4.0, mobility and nutrition.

SecuWeb is an Interreg France-Wallonie-Vlaanderen project under the coordination of TUA West in cooperation with CITC, Eurasanté, Howest, Idelux, Sirris, UCLouvain, UGent and UPHF.

Marwane Ayaida - Professor at Université Polytechnique Hauts- de-France

Emmelie Houzet - Project leader at TUA West

Day 2
Tuesday 03/12

08:30 AM – 09:00 AM
REGISTRATIONS

09:00 AM – 10:30 AM | Auditorium
Cybersecurity in our quantum age

Although practised as an art and science for ages, cryptography had to wait until the mid-twentieth century for Claude Shannon to endow it with a rigorous mathematical foundation. However, Shannon's approach was rooted in his own information theory, itself inspired by the classical physics of Newton and Einstein. Yet, the world in which we live is subject to the laws of quantum theory, no matter how bewildering, whose experimental verification half a century ago was rewarded in 2022 by the Nobel Prize in Physics. When quantum theory is taken into account, new vistas open up both for codemakers and codebreakers. Is this a blessing or a curse for cybersecurity? Quantum computers will soon be capable of computations that would be unthinkable for a conventional computer, which will seriously undermine the so-called security of Internet communications as we practise them today. Nevertheless, the same quantum theory gives rise to new cryptographic paradigms that are in principle invulnerable to arbitrary attacks, even by an adversary capable of harnessing unlimited computing power and technology. However, this unconditional security requires quantum cryptography to be implemented according to the theory, which is very challenging. Will the cat-and-mouse game between codebreakers and codemakers soon reach a decisive outcome? As we shall see, the jury is still out!

No prior knowledge in cryptography or quantum theory will be assumed. Please note that this talk will be given in French, with slides written in English.

Gilles Brassard - Professor of Montreal University

10:30 AM – 10:45 AM
COFFEE BREAK

09:00 AM – 10:30 AM | Auditorium
Cybersecurity in our quantum age

Although practised as an art and science for ages, cryptography had to wait until the mid-twentieth century for Claude Shannon to endow it with a rigorous mathematical foundation. However, Shannon's approach was rooted in his own information theory, itself inspired by the classical physics of Newton and Einstein. Yet, the world in which we live is subject to the laws of quantum theory, no matter how bewildering, whose experimental verification half a century ago was rewarded in 2022 by the Nobel Prize in Physics. When quantum theory is taken into account, new vistas open up both for codemakers and codebreakers. Is this a blessing or a curse for cybersecurity? Quantum computers will soon be capable of computations that would be unthinkable for a conventional computer, which will seriously undermine the so-called security of Internet communications as we practise them today. Nevertheless, the same quantum theory gives rise to new cryptographic paradigms that are in principle invulnerable to arbitrary attacks, even by an adversary capable of harnessing unlimited computing power and technology. However, this unconditional security requires quantum cryptography to be implemented according to the theory, which is very challenging. Will the cat-and-mouse game between codebreakers and codemakers soon reach a decisive outcome? As we shall see, the jury is still out!

No prior knowledge in cryptography or quantum theory will be assumed. Please note that this talk will be given in French, with slides written in English.

Gilles Brassard - Professor of Montreal University

12:15 PM – 01:15 PM
LUNCH TIME

01:15 PM – 02:00 PM | Auditorium
BeQCI and device-independent quantum key distribution

This presentation provides a brief introduction to the ***Belgian Quantum Communication Infrastructure (BeQCI) project***, part of the European EuroQCI initiative aimed at ***advancing secure* quantum communication networks across Europe**. *In addition to building infrastructure, BeQCI is driving research into future-proof quantum key distribution (QKD) protocols. Specifically, we will explore* **Device-Independent (DI) QKD**, *a cutting- edge approach to quantum cryptography that leverages* **Bell inequalities**, *recognized with the 2022 Nobel Prize in Physics. By eliminating certain security assumptions, DI QKD offers* **unprecedented levels of security** *beyond current QKD protocols. Attendees will gain insights into the* **future potential of DI and semi-DI QKD** *to enhance information security in the quantum era. Join us to discover how these advancements are* **pushing the boundaries of secure communication**.

Prof. Stefano Pironio - FRS-FNRS Research Director at ULB

02:00 PM – 02:45 PM | Auditorium

Eagle-1 : QKD in practice and build-up of users communities

The EAGLE-1 mission aims to develop Europe's first sovereign, **end-to-end space-based Quantum Key Distribution** *(QKD)* system. Led by SES in collaboration with the European Space Agency (ESA) and various European space agencies and private partners, the mission will feature a ***state-of-the-art QKD system*** comprising a payload aboard the EAGLE-1 ***Low Earth Orbit*** (LEO) satellite, ***optical ground stations, quantum operational networks***, and a ***key management system***. EAGLE-1 marks a significant milestone in next-generation quantum communication infrastructure, providing ***crucial technical insights*** and ***mission data*** while contributing to the ***EuroQCI program***'s development. It offers a unique ***opportunity*** for ***public and private*** entities to ***test and validate*** end-to-end Quantum Safe solutions through satellite-based QKD.

Thierry Draus - Vice President Business Development at SES

02:45 PM – 03:30 PM | Auditorium

Quantum Technologies for Communications Systems

In this talk, we will explore the exciting advancements in quantum technologies and their transformative impact on communication systems. Starting with an introduction to the ***Second Quantum Revolution***, we will delve into key developments, such as ***Quantum Communications Infrastructure*** and ***Quantum Key Distribution (QKD)***, which are poised to enhance data security and revolutionize the way we exchange information. Next, we will discuss the concept of the Quantum Internet, a futuristic network leveraging quantum principles for unprecedented communication capabilities. We will also cover ***Quantum Optimization*** techniques and their application to solving complex communication challenges, especially within large-scale and evolving networks like ***6G***. Finally, we will conclude with prespectives and open research problems offering a roadmap for the development and integration of quantum technologies in the years ahead.

Seid Koudia - Research Associate at University of Luxembourg

03:30 PM – 04:15 PM | Auditorium

FranceQCI and its challenges

We discuss current efforts towards ***the deployment of a national*** **quantum communication infrastructure** *in France. These include* technologies under development in our academic laboratories as well as benchmark demonstrations at the testbeds in operation *in the Paris and Nice regions* **involving industrial actors spanning the telecom operator, cybersecurity, QKD system provider,**
photonics and space sectors. We also discuss current challenges in the field of quantum communication and future perspectives.

Professor Eleni Diamanti - CNRS Research Director at Sorbonne University

04:15 PM – 04:30 PM

COFFEE BREAK

04:30 PM – 05:15 PM | Auditorium

INT-UQKD : cross-border QKD

Through a set of business-driven use cases, ***INT-UQKD*** ("International Use cases for Operational QKD Applications & *Services")* **will provide global quantum safe communication services upon a hybrid space-terrestrial quantum key distribution (QKD) backbone**. *By leveraging the* **QKD technology**, *together with other* **classical and post-quantum cryptographic protocols** *to deliver a practical environment that can be used in the current commercial context, INT-UQKD safeguards the secure exchange of information, the long-term protection of stored data, and the protection of critical infrastructure in the post quantum age.*

Thanks to its hybrid space and terrestrial network, ***INT-UQKD will demonstrate a global quantum safe communication between Redu (Belgium), Windhof (Luxembourg) and Singapore***. As ***INT-UQKD architecture is designed with scalability and interoperability mind***, it allows the incorporation of future extensions. These extensions will e***xpend both INT-UQKD*** **geographical reach and operational capabilities**, *aiming at* implementing a resilient, flexible and manageable ecosystem with ***global coverage enabling quantum secure communication*** and cryptographic services for private and governmental users.

Patrick Renaux - Senior cybersecurity architect

05:15 PM – 06:15 PM | Auditorium

Presentation of Quantum Demonstrator of GALAXIA in Transinne (Thales Belgium)

Jonathan Pisane - Innovation & Product Policy Manager at Thales Belgium

Day 3
Wednesday 04/12

9:00 AM – 9:30 AM
REGISTRATIONS

09:30 AM – 12:30 PM | Auditorium
Poster session (Abstract)

The ***3rd edition of the Cyberwal in Galaxia Program*** will feature an exciting ***poster competition*** where 30 posters will be showcased. The best poster will be honored with an ***Award***, which will be presented during the ceremony scheduled for ***Wednesday, 12/04***, in the late morning. An ***expert jury***, consisting of 10 professionals renowned in their fields, will select ***the winner*** of this Cybersecurity Award.

Beyond the competition, the poster session offers an exceptional opportunity for participants to ***present their innovative research and hone their scientific communication skills*** in front of a diverse audience, including business representatives.

This session is much more than a mere contest: it is ***a true exchange platform***. It enables participants to ***connect***, ***share ideas***, and ***enrich the international cybersecurity community***.

We warmly invite ***students, researchers***, and ***professionals*** to participate in this enriching event. Discover the ***latest innovations***, share ***your expertise***, and immerse yourself in an environment of ***collaboration and innovation***. Join us to ***celebrate excellence in cybersecurity*** and contribute to a tradition of ***impact*** and continuous ***progress***.

09:30 AM – 12:30 PM	***Introduction of the Poster session*** (overview, objectives, connecting of researchers with industries)
09:45 AM – 10:30 AM	***Elevator Pitch for 30 posters*** (1 minute per poster)
10:30 AM – 12:00 PM	***Poster session***
12:00 PM – 12:15 PM	***Presentation of CyberActive by Thierry Coutelier***
12:15 PM – 12:30 PM	***Awarding of the Best Poster & presentation by the winner***
12:30 PM	***End***

12:30 PM – 01:30 PM
LUNCH TIME

01:30 PM – 03:00 PM | Freedom & ISS
Introduction

A meticulously designed ***CTF challenge*** that push the boundaries of conventional cybersecurity knowledge. Attendees will be able to revel in the opportunity to listen to and interact with esteemed ***experts from the cybersecurity domain***, each bringing a wealth of experience and fresh perspectives.

Complementing these, our hands-on demonstrations promise ***a deep dive into the latest technologies and methodologies***, forging a link between academic theories and their tangible, real-world implementations. Join us for a comprehensive exploration of the future of cybersecurity.

Deloitte will invite keynotes speakers to develop on concise and insightful talk on a relevant cybersecurity topic and allow some time for questions and answers.

Nicolas Noël - Director, Cyber Risk Advisory at Deloitte
Etienne Caron - Manager, Cyber Risk Advisory at Deloitte

03:00 PM – 03:15 PM
COFFEE BREAK

03:15 PM – 04:45 PM | Freedom & ISS

A meticulously designed ***CTF challenge*** that push the boundaries of conventional cybersecurity knowledge. Attendees will be able to revel in the opportunity to listen to and interact with esteemed ***experts from the cybersecurity domain***, each bringing a wealth of experience and fresh perspectives.

Complementing these, our hands-on demonstrations promise ***a deep dive into the latest technologies and methodologies***, forging a link between academic theories and their tangible, real-world implementations. Join us for a comprehensive exploration of the future of cybersecurity.

Deloitte will invite keynotes speakers to develop on concise and insightful talk on a relevant cybersecurity topic and allow some time for questions and answers.

Nicolas Noël - Director, Cyber Risk Advisory at Deloitte
Etienne Caron - Manager, Cyber Risk Advisory at Deloitte

Day 4
Tuesday 05/12

08:30 AM – 09:00 AM
REGISTRATIONS

09:00 AM – 12:15 PM | ISS
An Introduction to Smart Contracts Security

This session focus on ***security*** aspect of modern financial transactions above blockchains: ***smart contracts***. To do so, the first part of the session will review key theoretical concepts, such as cryptography, hashing, signature, fingerprint, merkle tree) before diving into the notion of block chain and smart contracts. The ***Solidity*** programming language will be introduced and well known attacks will be discussed (e.g., reentrancy attack). In the second part of the session, attendees will have the opportunity to learn how to detect security breaches in smart contracts and how to abuse them for performing an attack.

Benoît Donnet - Professeur at Université de Liège

OR

09:00 AM – 09:45 AM | Auditorium
The blockchain landscape in Wallonia

Wallonia is active in the field of ***blockchain***, and a number of public and private initiatives are already underway. Before presenting some concrete projects implemented in our region, Nicolas Point will outline the two most important federative programs.

The ***WalChain*** initiative, which was born of a grouping of Walloon blockchain start-ups, aims to promote 'Made In Wallonia' blockchain as an innovative tool for building collaborative and transparent ecosystems, as well as an opportunity to contribute to sustainable economic redeployment in Wallonia. ***DigitalWallonia4.Trust*** is an innovative project led by Agoria, Infopole, Agence du Numérique and WalChain. Supported by the Service Public de Wallonie Economie Emploi et Recherche (SPW EER) and Wallonia, this initiative is part of the Digital Excellence program of Wallonia's digital strategy, Digital Wallonia. DW4TRUST aims to place Wallonia at the center of digital innovation. By integrating blockchain technology into various sectors, DW4TRUST not only improves efficiency, trust and security across businesses, but also opens up new opportunities for growth and innovation.

Nicolas Point - Responsable du département IT at MULTITEL
Aloïs Moubax - Program Manager at DigitalWallonia4.Trust

09:45 AM – 10:30 AM | Auditorium
Seamless Blockchain Integration: Transforming Existing Businesses with Innovative Solutions

This session will explore a proven methodology for integrating blockchain technology into existing business systems. We'll cover key steps, from assessing business needs and designing a tailored blockchain strategy, to implementing and deploying solutions that align with current infrastructure. Attendees will learn best practices for overcoming common challenges, such as data migration, interoperability, and security, while maximizing the benefits of blockchain, including transparency, efficiency, and trust. Real-world case studies will highlight successful integrations in sectors like supply chain, ESG reporting, and Digital Product Passports (DPP).

Harold Kinet - CEO at BE Blockchain

10:30 AM – 10:45 AM
COFFEE BREAK

10:45 AM – 11:45 AM | Auditorium
Logion: Blockchain and IPFS to Secure and Certify Sensitive Data

In a world where digital threats are rapidly evolving, the need for advanced solutions to secure sensitive data is paramount. Logion offers an innovative approach by combining ***blockchain technology with IPFS*** (InterPlanetary File System). This combination not only ensures the integrity and traceability of data but also guarantees its availability and immutability. Blockchain, with its ***decentralized nature***, provides an unalterable and transparent ledger, while IPFS enables distributed and resilient file storage. Together, these technologies offer a ***robust alternative to traditional storage*** solutions, meeting the increasing demands for security in cyberspace. This session will explore how Logion leverages these technologies to provide ***superior protection for sensitive data***, particularly in sectors where confidentiality and security are crucial. Participants will learn how the combination of blockchain and IPFS can not only enhance data security but also facilitate certification and traceability, all while adhering to the strictest privacy standards.

David Schmitz - Founder of Logion
Gérard Dethier - CTO at Logion

11:45 AM – 12:15 PM | Auditorium

The Future of Blockchain and Web3 in Wallonia

Moderator: Aloïs Moubax - *Program Manager at* DigitalWallonia4.Trust
Moderator: Nicolas Point - Head of the IT Department
David Schmitz - Founder of Logion
Gérard Dethier - CTO at Logion
Harold Kinet - CEO at BE Blockchain

12:15 PM – 01:15 PM
LUNCH TIME

01:15 PM – 04:15 PM | ISS

An Introduction to Smart Contracts Security

This session focus on ***security*** aspect of modern financial transactions above blockchains: ***smart contracts***. To do so, the first part of the session will review key theoretical concepts, such as cryptography, hashing, signature, fingerprint, merkle tree) before diving into the notion of block chain and smart contracts. The ***Solidity*** programming language will be introduced and well known attacks will be discussed (e.g., reentrancy attack). In the second part of the session, attendees will have the opportunity to learn how to detect security breaches in smart contracts and how to abuse them for performing an attack.

Benoît Donnet - Professeur at Université de Liège

OR

01:15 PM – 02:30 PM | Auditorium

Emerging ICT trends: the need for secure and quantum-safe networks

We will highlight the increasing need to have strong network security resulting from the adoption of new technologies like AI, 5G, IoT and quantum. We will review the different network security technologies available on offer today. And we will explore the impact of crypto-relevant quantum computers on organisations, and how you can already prepare today.

Wim Van Vossel - Proximus NXT

02:30 PM – 03:30 PM | Auditorium

AI-enabled disconnected sovereign cloud in Luxembourg for Europe

Clarence's core mission is to offer a cutting-edge, disconnected sovereign cloud solution. Based on Google Cloud technology, this unique proposition guarantees the confidentiality and security of the most sensitive information, giving control over data, and offering total autonomy of operation. Clarence respects the highest ethical standards in data protection, confidentiality, transparency and regulatory compliance.

Clarence is the result of a joint venture between Proximus and LuxConnect. A joint venture born of the desire to create a disconnected sovereign cloud, designed to meet the needs of companies wishing to retain control over the integrity of their data and access to it, but also, operationally, to ensure that their operations are carried out on our soil and subject only to European jurisdictions.

The origins of Clarence lie in a shared ambition: to offer users the most advanced Cloud functionalities, while guaranteeing them total control over where their data resides and who has access to it.

What We Do : Combining Innovation and Sovereignty in Cloud Computing

The sovereign cloud solves the dilemma between innovation and compliance. By combining the best of both worlds, it facilitates access to technological innovations while ensuring compliance and protection of sensitive data.

Pascal Rogiest - General Manager at Clarence S.A.

03:30 PM – 03:45 PM
COFFEE BREAK

03:45 PM – 04:45 PM | Auditorium

Cloud Continuum Security Challenges

EU IPCEI on Next Generation Cloud Infrastructure and Services

Cloud & edge computing are crucial for an interconnected and resilient Digital Europe, as well as for the EU's geostrategic position and competitiveness in the global economy. IPCEI CIS is the first IPCEI in the cloud and edge computing domain. It concerns the development of ***the first interoperable and openly accessible European data processing ecosystem***, the multi-provider cloud to edge continuum. It will ***develop data processing capabilities, and software and data sharing tools*** that enable federated, energy-efficient and trustworthy cloud and edge distributed data processing technologies and related services. The innovation provided by IPCEI CIS will enable a new spectrum of possibilities for ***European businesses and citizens***, advancing the Digital and Green transition in Europe.The main aim of the session is to introduce the main cloud continuum ***security challenges focusing on relevant topics like Confidential Computing, ultra-high resilience, cloud certification***, etc.

Jordi Guijarro - Principal Technologist at Cloud-Edge Innovation

04:45 PM – 05:30 PM | Auditorium

A Tale of Vulnerability Prediction

Over the past years, automated vulnerability prediction research, mainly supported by AI techniques, has grown in popularity. While a large number of studies have been proposed, they often make simplification assumptions, which limit their applicability and adoption. This talk will provide a historical view of the vulnerability prediction approaches and will focus on the challenges and limitation that they face through the lens of three different research communities, i.e., AI, SE and Security. The talk will conclude with a discussion on the links between vulnerability prediction and testing, showing potential applications and cross-fertilization between the two research fields.

Mike Papadakis - Associate Professor at SnT

05:30 PM – 06:00 PM | Auditorium

How sovereign cloud solutions contribute to European digital autonomy?

Moderator: Pascal Rogiest - General Manager at Clarence S.A.
Wim Van Vossel - Proximus NXT.
Jordi Guijarro - Principal Technologist at Cloud-Edge Innovation
Mike Papadakis - Associate Professor at SnT

07:00 PM | Hub

Aperitif

Day 5
Friday 06/12

09:00 AM – 10:00 AM
REGISTRATIONS

09:00 AM – 10:00 AM | Auditorium
Innovation and judicial police: a winning combination in the fight against crime

The Federal Judicial Police will present its overall vision and the role of technology in achieving it.

The main drivers of our strategy will be outlined to explain their use in our digital transformation and the disruption of our operational processes.

We will provide concrete examples of technological achievements in operations where an inclusive approach has been a key factor in success.

We will then discuss the challenges of operational Big Data and the contribution of AI to our complex processes.

David JAROSZEWSKI - Senior advisor on digital transformation and innovation

10:00 AM – 11:15 AM | Auditorium
Introduction – The hack of the city of Antwerp and lessons learned (Amphi)

After a brief introduction to the current ransomware landscape, we review the case of the City of Antwerp based on information that was published by the city and in the press over the course of the attack and the months that followed – looking at the IT, operational, communication, reputation and financial impacts of the attack. The presentation is organized as a timeline of events, supported with press clippings and public facts brought ttogether into an exciting story that unravels over time

Didier Stevens - Senior Analyst at NVISO
Vincent Defrenne - Partner, Cyber Strategy & Architecture at NVISO

11:15 AM – 11:30 AM
COFFEE BREAK

11:30 AM – 01:00 PM | Auditorium
Crisis response exercise: the enemy from within (2 rooms)

Participants take the helm of the crisis management team of a fictitious energy producer running its operations across Eastern Europe, and are confronted with a rapidly evolving incident involving the compromission of some of their systems and the potential involvement of an internal system administrator in these activities. The exercise is organized as a succession of briefings from the incident response team and analysis in group to define together a course of action that responds to the events and the questions raised. The response of course consists of technical actions to analyse, isolate, contain and eradicate the threat, but also involves organizational measures and measures in terms of internal and external communication. The exercise is facilitated by seasoned crisis and incident responders Vincent Defrenne and Didier Stevens.

Didier Stevens - Senior Analyst at NVISO
Vincent Defrenne - Partner, Cyber Strategy & Architecture at NVISO

01:00 PM – 02:00 PM
LUNCH TIME

02:00 PM – 05:00 PM | Auditorium

Ransomware Workshop (2 rooms)

During the workshop, participants will learn how to deal with this situation step-by-step by challenging them in their knowledge of various infosecurity topics. The goal of this workshop is to provide the participants with a structured approach on how to spot malware and how to deal with incidents caused by modern adversaries. Instructors will be assisting the students towards the full mapping of the incident and will provide a typical solution at the end of the workshop. The situation that the students will have to handle is as follows: “You are part of your company’s Incident Response team. On some idle Friday afternoon, your manager barges in. He has just been notified by the authorities that they have compromised a Commandand-Control server and that they have found systems communicating to that server originating from your company. The board of directors is breathing down his neck to find out what has happened and has asked him to contain this problem as soon as possible. How come we haven’t noticed this? What systems have been compromised? What data is exfiltrated?
Are there still active connections? You immediately coordinate with the authorities and receive an extract of the information they have pulled from the compromised server. And so you quest begins…” The students will work in teams of 2 and will have 4 hours to find out what has happened and to verify if there is still any active connections. During the workshop, the instructors will switch between guiding the participants and challenging them by assuming various positions in the company. The workshop will start with the set up of the participants machines with the tools required. For those participants that may not install such tools on their machine, a Linux-based virtual machine will be available for download or on USB sticks.

Didier Stevens - Senior Analyst at NVISO
Vincent Defrenne - Partner, Cyber Strategy & Architecture at NVISO

05:00 PM

The end

Cette école, fruit de l’ambition d’**IDELUX et de ses partenaires**, aspire à devenir un **centre de formation européen** de premier plan pour répondre aux besoins spécifiques des institutions, des entreprises et de la société civile.

Cette troisième édition est une nouvelle fois un franc succès et témoigne également de la **reconnaissance internationale de l'expertise belge en matière de cybersécurité**.

L’avenir de cette école est assuré puisque **les éditions 2025 et 2026 sont déjà en préparation**.
D’une durée d’**une semaine**, les étudiants seront encadrés par des intervenants des mondes académique, industriel et public, belges et étrangers, triés sur le volet.

Le renforcement de Cyberwal à Galaxia positionne ainsi **la province de Luxembourg** en acteur clé de la cybersécurité en Belgique.
Avec une vision claire et une expansion rapide, **IDELUX et Cyberwal by Digital Wallonia** s'emploient à positionner la Wallonie comme un leader mondial de la cybersécurité, alignant les éditions futures du programme « Cyberwal in Galaxia » avec les standards européens d'excellence et répondant aux exigences croissantes de l'écosystème cyber international.

Objectifs du Plan de relance de la Wallonie en cybersécurité :

- **Renforcer** la souveraineté numérique.
- **Protéger** les citoyens et les entreprises.
- **Valoriser** la recherche.
- **Développer** des outils stratégiques accessibles à tous.

Mesures mises en œuvre par le Gouvernement :

- Création d'une chaîne de valeur « cybersécurité » complète : **sensibilisation, information, formation, outillage et recherche.**

Initiative Cyberwal by Digital Wallonia :

- Mise en place, à Galaxia, d'une **structure regroupant recherche, entreprises et enseignement.**
- **Centralisation** de l'accès aux outils de pointe.
- **Mise en relation** des citoyens, entreprises et pouvoirs publics avec des experts locaux et internationaux.

Exemple concret :

- Une entreprise peut simuler une cyberattaque, évaluer son niveau de maturité et accéder à des solutions adaptées grâce à ce **pôle d'excellence.**

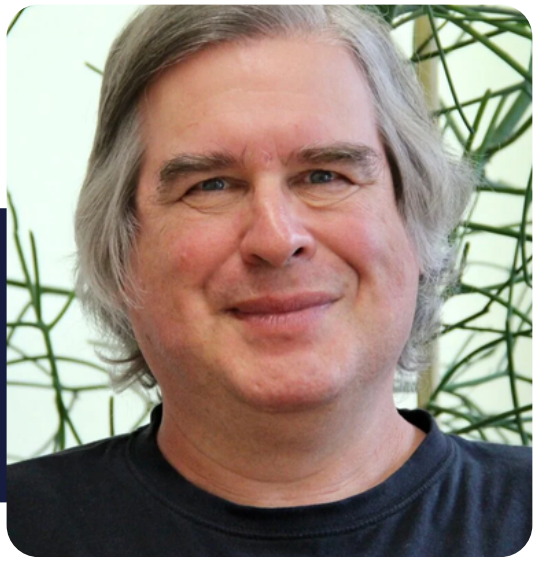
La Cybersécurité quantique : conférence du Professeur Gilles Brassard

La cybersécurité quantique est un domaine émergent qui explore l'impact de l'informatique quantique sur la sécurité des systèmes numériques, offrant des opportunités immenses.

Notre existence quantique représente-t-elle une bénédiction ou une malédiction pour la sécurité informatique ?

Les ordinateurs quantiques, avec leur **capacité à effectuer des calculs inimaginables pour un ordinateur conventionnel**, risquent de compromettre la sécurité des communications sur Internet telle que nous la connaissons aujourd'hui. Paradoxalement, cette même théorie quantique ouvre la porte à une **cryptographie théoriquement invulnérable**, résistante à toute puissance de calcul ou technologie d'espionnage. Cependant, sa mise en œuvre correcte reste un défi de taille. Le jeu du chat et de la souris entre sécurité et espionnage est-il sur le point de connaître son dénouement ? À ce jour, la réponse demeure incertaine.

Gilles Brassard est une **figure emblématique de la cryptographie et de la sécurité quantiques**. Professeur d'informatique à l'Université de Montréal depuis 1979, Gilles Brassard a jeté les bases de la cryptographie quantique à une époque où personne ne pouvait prévoir que les technologies quantiques allaient devenir une industrie se chiffrant maintenant en milliards de dollars par année.



Il est aussi parmi les inventeurs de la téléportation quantique, considérée internationalement comme pilier fondamental de l'informatique quantique.

Ses contributions révolutionnaires

- **Cryptographie quantique** : avec son collaborateur Charles Bennett, Gilles Brassard a développé en 1984 le protocole BB84, qui reste à ce jour la méthode la plus connue et la plus utilisée pour la distribution quantique de clés (QKD). Ce protocole exploite les lois fondamentales de la mécanique quantique pour créer des communications inviolables.

- **Téléportation quantique** : co-inventeur de ce concept en 1993, il a ouvert la voie à des applications révolutionnaires dans la transmission de l'information à distance.

- **Reconnaissance mondiale** : ses contributions lui ont valu des distinctions prestigieuses, telles que :

    - Fellow de la Royal Society de Londres et membre international de la National Academy of Sciences des États-Unis, officier de l'Ordre du Canada et de l'Ordre national du Québec
    - Le **Prix Wolf** en physique
    - Le prix Micius Quantum
    - Le BBVA Foundation Frontiers of Knowledge Award in Basic SciencesII
    - Le Prix Breakthrough en physique fondamentale (2023), un honneur rare dans le domaine scientifique.
    - Doctorats honorifiques de l'ETH Zürich, de l'Université d'Ottawa et de l'Università della Svizzera italiana de Lugano.
    - Un rôle central dans la popularisation de la science quantique auprès d'un large public.

Gilles Brassard est non seulement un pionnier scientifique, mais aussi un **vulgarisateur passionné**, rendant accessibles des concepts complexes à des audiences variées.

Conférence : La sécurité informatique à l'ère quantique (conférence en français)

Le 3 décembre 2024, Gilles Brassard animera une conférence exceptionnelle à l'Euro Space Center de Transinne. Cette intervention sera l'occasion d'explorer comment la théorie quantique redéfinit les enjeux de la cybersécurité.

Pourquoi cette conférence est unique

- **Un visionnaire au cœur de la transition technologique** : Gilles Brassard, en tant que fondateur de la cryptographie quantique, est la voix la plus autorisée pour aborder l'impact des ordinateurs quantiques sur nos systèmes de sécurité actuels.
- **Accessibilité et clarté** : bien qu'il s'agisse d'un domaine complexe, Brassard s'assure de vulgariser ses explications pour que même les non-initiés puissent comprendre les enjeux.
- **Impact concret** : il démontrera comment les technologies quantiques pourraient révolutionner la sécurité informatique, tout en identifiant les défis à surmonter pour leur adoption.

Programme et informations clés

- **Date : Mardi 3 décembre 2024**
- **Horaire : De 9h00 à 12h15 (pause de 10h30 à 10h45)**
- **Lieu : Euro Space Center, Devant les Hêtres, 1 – 6890 Libin**

Gilles Brassard : une source d'inspiration

Ce n'est pas seulement une conférence, mais une rencontre avec l'un des esprits les plus brillants de notre époque. Que vous soyez novice ou expert en cybersécurité, cette session vous permettra de plonger dans l'univers fascinant des technologies quantiques, avec l'éclairage unique de Gilles Brassard, un véritable architecte du futur numérique.

A propos d'IDELUX

Le Groupe IDELUX est l'**Agence de développement territorial en province de Luxembourg.**

Il est actif dans quatre grands domaines : le développement économique, l'accompagnement des communes dans le montage de leurs projets, la gestion de l'eau et celle des déchets.

Constitué de cinq intercommunales, sa mission d'intérêt général consiste à « **contribuer à l'amélioration du bien-être de la population sur le territoire desservi** ».

Parmi les secteurs économiques prioritaires pour IDELUX, **le spatial est stratégique** avec l'implantation d'un des 7 centres opérationnels de l'Agence Spatiale Européenne (ESA) à Redu en province de Luxembourg. Le rôle d'IDELUX est de **créer un véritable écosystème cybersécurité autour de Redu-Galaxia** (Transinne), parc d'activités économiques dédié au spatial et aux hautes technologies, géré par l'Intercommunale.

Concrètement, **l'ESA, avec qui IDELUX a des relations étroites**, a mis en place son centre de connaissances ainsi que son Cyber Security Operation Center afin de pouvoir assurer, essentiellement depuis Redu, les opérations cybersécurité au sol et en vol de l'Agence.

Forte de son engagement dans ce secteur prioritaire, **IDELUX a soutenu l'initiative « Cyberwal »** qui réunit l'ensemble des acteurs wallons impliqués dans la cybersécurité.

C'est donc dans le contexte de Cyberwal que s'organise cette troisième édition de l'école internationale dédiée à la cybersécurité.

Cette école s'inscrit dans le cadre d'un **financement du Plan de relance wallon**, et a été soutenue par le Ministre Willy Borsus, et aujourd'hui par le Ministre Pierre-Yves Jeholet.

En résumé

VOICI LES PRINCIPALES ÉTAPES DE LA POLITIQUE WALLONNE DE CYBERSÉCURITÉ :

- Mise en place d'un **pôle dédié à la cybersécurité** avec une structure de gouvernance adaptée.
- **Soutien financier** pour les acteurs impliqués dans la recherche en cybersécurité.
- **Sensibilisation** des citoyens, entreprises et institutions publiques aux enjeux de la cybersécurité.
- **Formation spécifique** destinée aux particuliers, entreprises et pouvoirs publics.
- **Développement d'outils et services avancés** pour renforcer la protection.
- **Création et activation d'un point de contact unique** pour centraliser les démarches.

L'inauguration de la **première École internationale dans le cadre de l'initiative Cyberwal** et l'organisation de sa troisième édition s'alignent parfaitement avec la stratégie européenne de cybersécurité, visant à **accroître la résilience** de l'Europe et de ses États membres face aux cybermenaces.

Cette école, en plus de symboliser un engagement éducatif fort, joue un **rôle crucial dans le développement d'un écosystème robuste dédié à la cybersécurité en Wallonie.** En rassemblant les compétences, les forces et les talents des acteurs régionaux, elle positionne la Wallonie comme un **acteur majeur dans l'élaboration de solutions de cybersécurité à l'échelle européenne.**

Grâce à cette initiative, la Wallonie contribue activement à **renforcer le réseau de connaissances** et de compétences essentielles pour répondre efficacement aux défis sécuritaires du numérique en Europe.

CONTACTS

Nous nous ferons un plaisir de vous accueillir le **mardi 3 décembre dès 13h30 à l'Euro Space Center**.

N'hésitez pas à nous contacter pour toute question ou demande d'interview.

Adresse du jour : Devant les Hêtres, 1 à B-6890 Libin

Relations presse

Isabelle Damoisaux-Delnoy	idd@iddup.be +32 474 74 13 31
Sylvie Adant	sylvie.adant@idelux.be +32 496 21 24 08

Plus d'informations

www.cyberwalingalaxia.be