BỘ TÀI NGUYÊN VÀ MÔI TRƯỜNG
TỔNG CỤC MÔI TRƯỜNG

# TRÍ TUỆ NHÂN TẠO (AI) VÀ AN NINH MẠNG (CYBERSECURITY)

**Ths. Nguyễn Xuân Thủy, Phó Giám đốc**
**Trung tâm Thông tin và Dữ liệu môi trường**

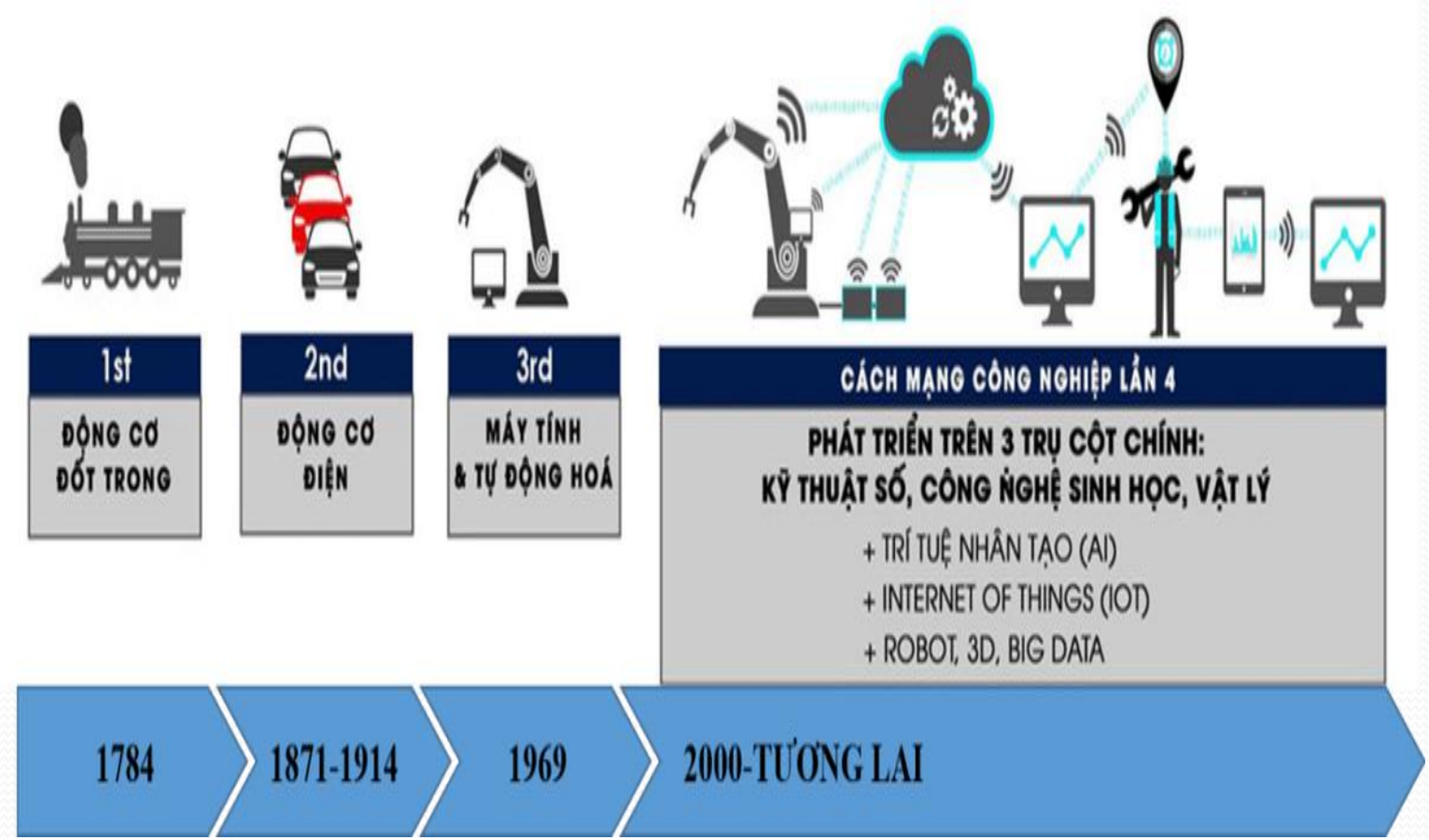
TP. Hải Phòng, 8.2022

# NỘI DUNG TRÌNH BÀY

1. Mở đầu
2. Các văn bản pháp lý
3. Trí tuệ nhân tạo (Artificial Intelligence)
4. An ninh mạng (Cybersecurity)
5. Trí tuệ nhân tạo và An ninh mạng
6. Kết luận

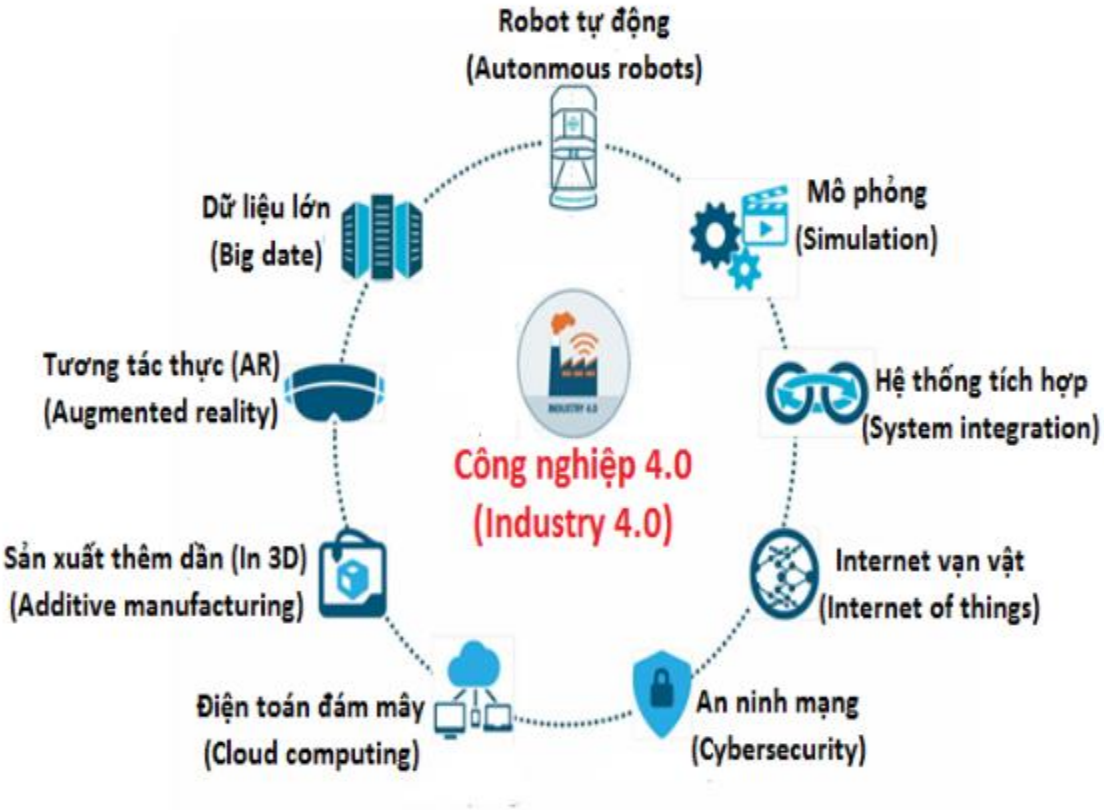
# MỞ ĐẦU

## 1. CMCN 4.0



# MỞ ĐẦU

## 2. Kỹ thuật số trong CMCN 4.0

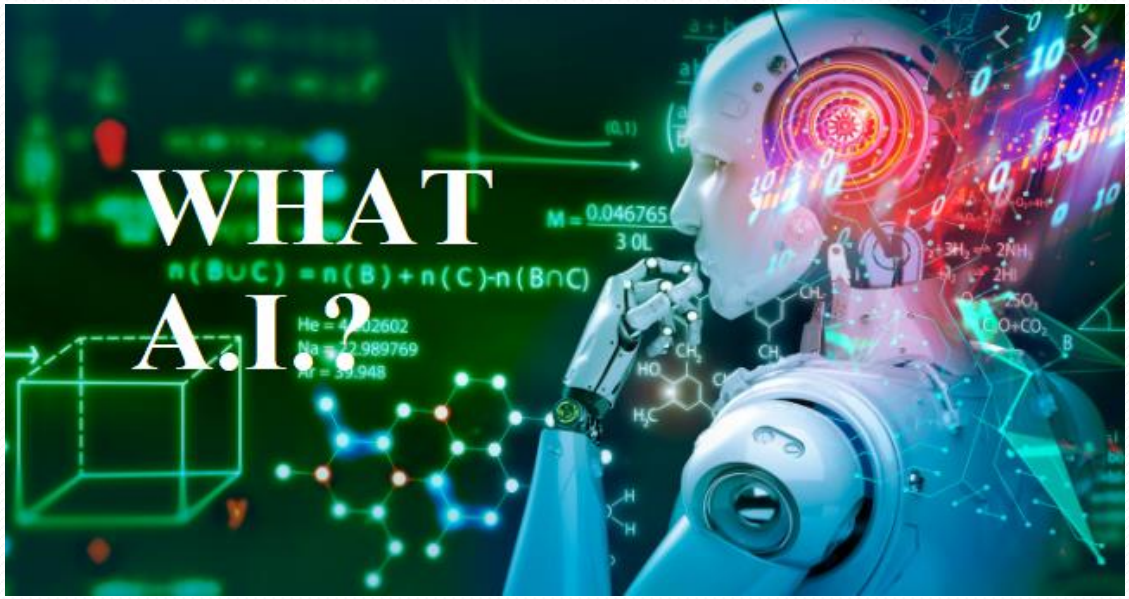


# VĂN BẢN PHÁP LÝ

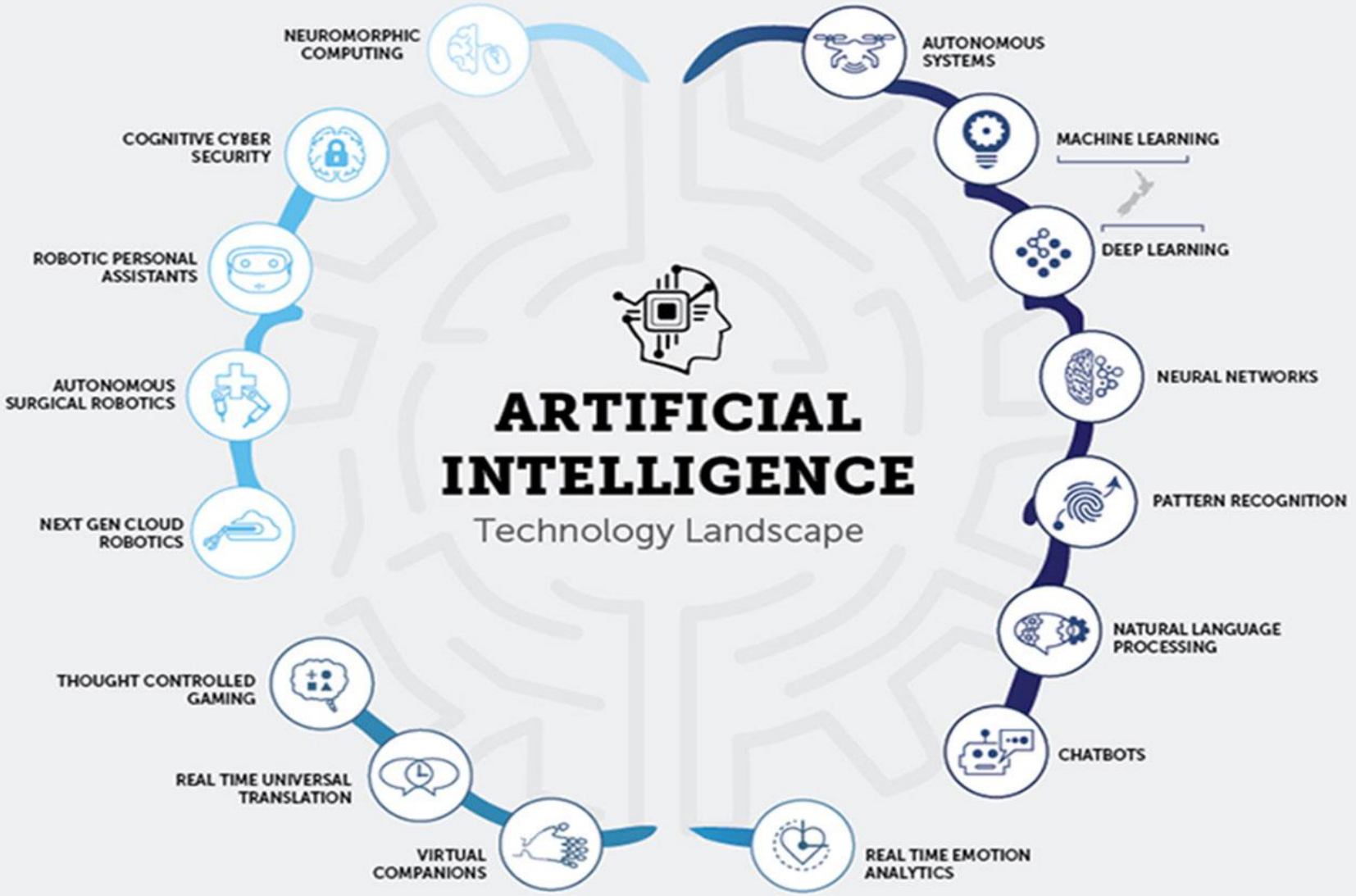
- Các VBQPPL về CMCN 4.0, ứng dụng CNTT, xây dựng Chính phủ điện tử, chuyển đổi số, đảm bảo an toàn hệ thống thông tin theo cấp độ, an toàn an ninh mạng.
- Quyết định số 127/QĐ-TTg ngày 26 tháng 01 năm 2021 của Thủ tướng Chính phủ Ban hành Chiến lược quốc gia về nghiên cứu, phát triển và ứng dụng Trí tuệ nhân tạo đến năm 2030.
- Quyết định 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng phê duyệt Chiến lược An toàn, An ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn 2030.

# TRÍ TUỆ NHÂN TẠO (AI)

**1. Khái niệm:** Trí tuệ nhân tạo (AI) Là trí tuệ do con người lập trình tạo nên với mục tiêu giúp máy tính có thể tự động hóa các hành vi thông minh như con người. Cụ thể, trí tuệ nhân tạo giúp máy tính có được những trí tuệ của con người như: biết suy nghĩ và lập luận để giải quyết vấn đề, biết giao tiếp do hiểu ngôn ngữ, tiếng nói, biết học và tự thích nghi…



# TRÍ TUỆ NHÂN TẠO (AI)



# TRÍ TUỆ NHÂN TẠO (AI)

## 2. Các loại AI

**2.1. Công nghệ AI phản ứng:** có khả năng phân tích những động thái khả thi nhất của chính mình và của đối thủ, từ đó, đưa ra được giải pháp tối ưu nhất.

# TRÍ TUỆ NHÂN TẠO (AI)

**2. Các loại AI**

**2.2. Công nghệ AI với bộ nhớ hạn chế:** Đặc điểm là khả năng sử dụng những kinh nghiệm trong quá khứ để đưa ra những quyết định trong tương lai. Công nghệ AI này thường kết hợp với cảm biến môi trường xung quanh nhằm mục đích dự đoán những trường hợp có thể xảy ra và đưa ra quyết định tốt nhất cho thiết bị.

# TRÍ TUỆ NHÂN TẠO (AI)

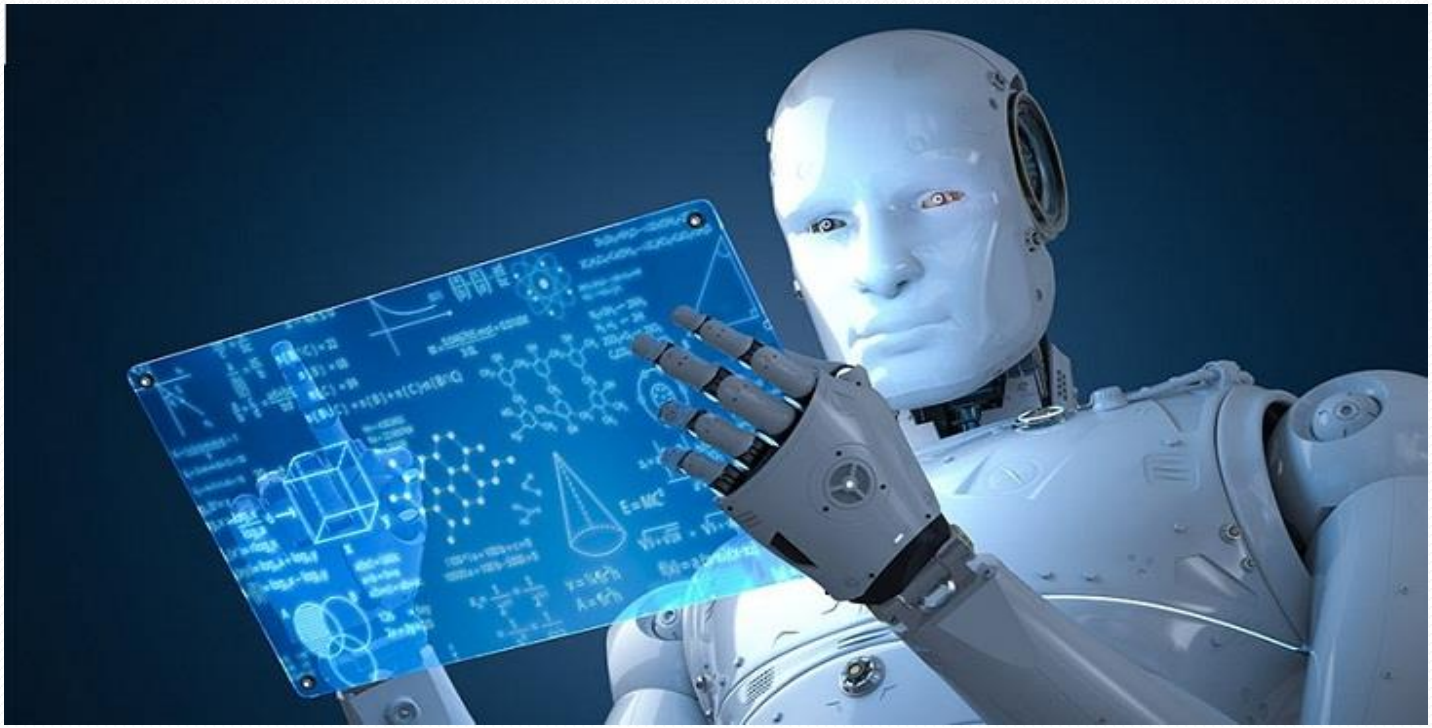
**2. Các loại AI**

**2.3. Lý thuyết trí tuệ nhân tạo:** Công nghệ AI này có thể học hỏi cũng như tự suy nghĩ, sau đó áp dụng những gì học được để thực hiện một việc cụ thể. Ví dụ: AI do Facebook tạo ra nhằm hỗ trợ giao tiếp kỹ thuật số được tốt hơn, nhưng không thực hiện được do AI tạo ra các ngôn ngữ mà con người không hiểu được.

# TRÍ TUỆ NHÂN TẠO (AI)

**2. Các loại AI**

**2.4. Tự nhận thức:** Công nghệ AI này có khả năng tự nhận thức về bản thân, có ý thức và hành xử như con người. Thậm chí, chúng còn có thể bộc lộ cảm xúc cũng như hiểu được những cảm xúc của con người. Đây được xem là bước phát triển cao nhất của công nghệ AI và đến thời điểm hiện tại, công nghệ này vẫn chưa khả thi.



# TRÍ TUỆ NHÂN TẠO (AI)

**2. Các loại AI**

**2.5 .Trí tuệ nhân tạo hẹp (ANI):** Trí thông minh nhân tạo hẹp đề cập đến các hệ thống AI chỉ có thể thực hiện một nhiệm vụ cụ thể một cách tự động bằng cách sử dụng các khả năng giống như con người. Ví dụ: các trợ lý ảo cá nhân như Google Assistant, nguồn cấp tin tức của Facebook, các đề xuất sản phẩm của Amazon

# TRÍ TUỆ NHÂN TẠO (AI)

**2. Các loại AI**

**2.6. Trí tuệ nhân tạo tổng hợp (AIG):** có ý thức, suy nghĩ khách quan, khả năng tự nhận thức, tri giác và sự khôn ngoan. AGI còn được gọi là AI mạnh và có trí thông minh ngang bằng với trí tuệ của con người.

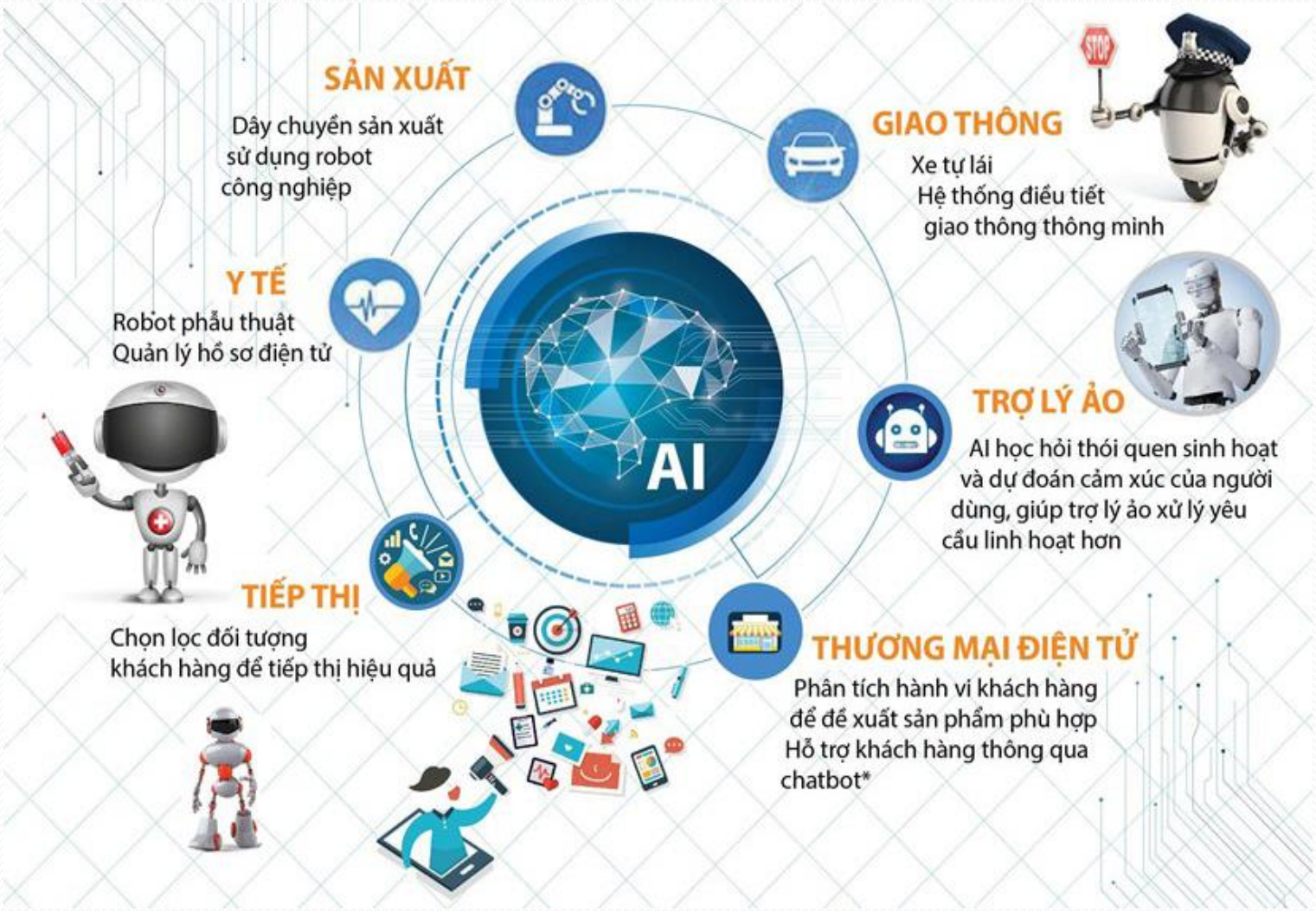
# TRÍ TUỆ NHÂN TẠO (AI)

**2. Các loại AI**

**2.7. Siêu trí tuệ nhân tạo** (ASI): Siêu AI là nơi máy móc vượt qua khả năng trí tuệ và khả năng nhận thức của con người. Một khi chúng ta mở khóa ASI, máy móc sẽ có khả năng dự đoán cao hơn và sẽ có thể suy nghĩ theo cách mà con người không thể hiểu được.

# TRÍ TUỆ NHÂN TẠO (AI)

## 3. Ứng dụng AI trong cuộc sống hiện tại và tương lai



# TRÍ TUỆ NHÂN TẠO (AI)

## 3. Ứng dụng AI trong cuộc sống hiện tại và tương lai

**Trong giáo dục**: AI giúp tạo ra những thay đổi lớn trong lĩnh vực giáo dục. Các hoạt động giáo dục như chấm điểm hay dạy kèm học sinh có thể được tự động hóa nhờ công nghệ AI. Nhiều trò chơi, phần mềm giáo dục ra đời đáp ứng nhu cầu cụ thể của từng học sinh, giúp học sinh cải thiện tình hình học tập theo tốc độ riêng của mình.

**Trong lĩnh vực tài nguyên môi trường**

- Nghiên cứu xây dựng công nghệ nền tảng trí tuệ nhân tạo phục vụ chuyển đổi số ngành tài nguyên và môi trường

- Nghiên cứu ứng dụng trí tuệ nhân tạo và viễn thám phục vụ giám sát thực hiện quy hoạch sử dụng đất.

- Nghiên cứu cơ sở khoa học và thực tiễn kết hợp công nghệ Georadar, công nghệ định vị RTK và Trí tuệ nhân tạo (AI) trong thành lập bản đồ công trình ngầm 3D phục vụ quá trình chuyển đổi số dữ liệu về bản đồ công trình ngầm.

# AN NINH MẠNG (CYBERSECURITY)

**1. An ninh mạng là gì?**

- **An ninh mạng (Cyber Security):** là hành động bảo vệ máy tính, máy chủ, các thiết bị di động, hệ thống điện tử, mạng và dữ liệu khỏi những tấn công độc hại. An ninh mạng cũng được biết đến như đảm bảo an ninh công nghệ hoặc thông tin điện tử.

# AN NINH MẠNG (CYBERSECURITY)

## 1. An ninh mạng là gì?

- **Bảo mật mạng (Network Security)** là thuật ngữ mô tả việc bảo vệ mạng máy tính khỏi những kẻ xâm nhập, dù là tấn công có mục đích hoặc những phần mềm độc hại gây rối.
- **Bảo mật ứng dụng (Application Security)** tập trung vào việc ngăn chặn các phần mềm hoặc thiết bị khỏi những đe dọa bên ngoài.
- **Bảo mật thông tin (Information Security)** là bảo vệ tính an toàn và riêng tư của dữ liệu, kể cả trong lưu trữ và chuyển đổi.
- **Bảo mật hoạt động (Operational Security)** bao gồm các quy trình và quyết định xử lý để giải quyết và bảo vệ tài sản dữ liệu. Các quyền truy cập mạng của người dùng, những phương thức xác định vị trí và cách thức dữ liệu được lưu trữ hoặc chia sẻ trong vùng quyền này.
- **Phục hồi sau thảm họa và tiếp tục hoạt động** là việc các tổ chức phản ứng với một sự cố an ninh mạng hoặc bất kì sự kiện nào dẫn đến việc mất dữ liệu hoặc không thể hoạt động.
- **Giáo dục người dùng cuối (End-user Education)** nói đến yếu tố khó lường nhất của an ninh mạng: con người. Bất cứ ai cũng có thể vô tình mang virus đến một hệ thống máy tính chỉ vì không tuân theo những bước bảo đảm an toàn. Chỉ cho người dùng cách xóa những email chứa  tệp đính kèm đáng nghi, hoặc không cắm ổ USB không xác định nguồn gốc là một trong nhiều bài học quan trọng giúp bảo đảm an ninh mạng cho mọi tổ chức và cá nhân.

# AN NINH MẠNG (CYBERSECURITY)

## 2. Quy mô các mối đe dọa an ninh mạng

- Các mối đe dọa an ninh mạng trên toàn cầu vẫn tiếp tục tăng nhanh với số lượng vi phạm dữ liệu nhiều hơn hàng năm.
- Dịch vụ y tế, bán lẻ và những thực thể công là những thành phần gặp phải nhiều vi phạm nhất, hầu hết những tội phạm tinh vi đều tấn công vào các lĩnh vực này. Sở dĩ chúng thu hút tội phạm vì dữ liệu tài chính và y tế rất dễ dàng thu thập được qua mạng, nhằm mục tiêu gián điệp hoặc tấn công khách hàng.
- Vì quy mô đe dọa an ninh mạng ngày càng tăng, Tập đoàn Dữ liệu Quốc tế (IDG) đưa ra dự đoán đến năm 2022, cả thế giới sẽ đối mặt với số tiền khổng lồ để giải quyết những tình trạng vi phạm: 133.7 tỉ đô la Mỹ. Các chính phủ trên toàn cầu đều ra sức giúp đỡ các doanh nghiệp tạo lập hệ thống an ninh mạng một cách hiệu quả nhất.

# AN NINH MẠNG (CYBERSECURITY)

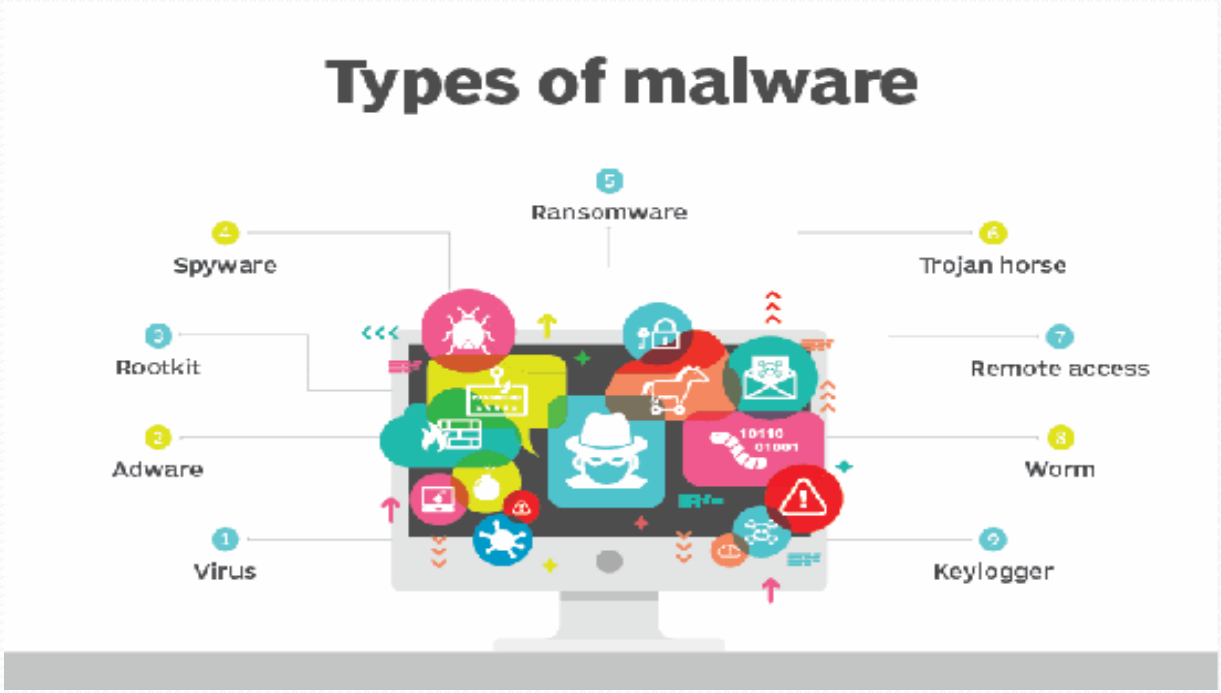
**3. Các mối đe dọa an ninh mạng**

- **Tội phạm mạng (Cybercrime)**: bao gồm cá nhân hoặc nhóm tội phạm nhằm mục tiêu tài chính hoặc muốn đánh sập một hệ thống (đôi khi là cả hai).
- **Tấn công mạng (Cyberattack)**: thường liên quan đến những động cơ về chính trị.
- **Khủng bố mạng (Cyberterrorism)**: mục tiêu thường là phá hỏng hệ thống điện tử gây hoảng loạn và sợ hãi.

# AN NINH MẠNG (CYBERSECURITY)

**4. Những phương pháp có thể đe dọa đến an ninh mạng**

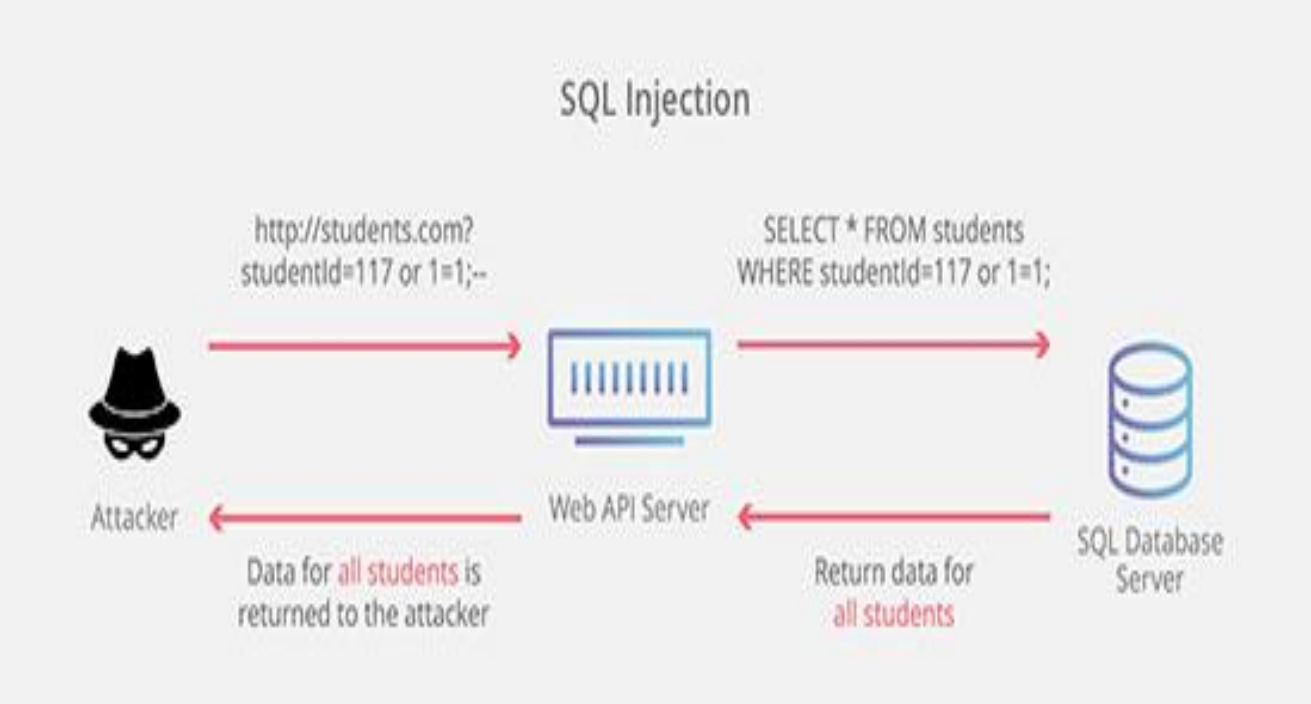
**4.1. Malware - Phần mềm độc hại:** Malware là một trong những mối đe dọa phổ biến nhất. Nó là một phần mềm được các tội phạm mạng tạo ra để ngăn chặn hoặc phá hủy máy của một người dùng. Malware thường được phát tán dưới dạng tệp đính kèm trong email hoặc những phần mềm "trông có vẻ an toàn". Malware được các tên tội phạm sử dụng cho mục đích kiếm tiền hoặc các động cơ chính trị, hướng đến việc tạo ra các cuộc tấn công mạng.



# AN NINH MẠNG (CYBERSECURITY)

**4. Những phương pháp có thể đe dọa đến an ninh mạng**

**4.2. SQL Injection:** cho phép những kẻ tấn công kiểm soát và đánh cắp dữ liệu từ cơ sở dữ liệu. Hacker khai thác những lỗ hổng dựa trên dữ liệu của ứng dụng, chèn mã độc thông qua những câu lệnh SQL vào hệ thống. Chúng có thể truy cập vào những thông tin nhạy cảm có trong cơ sở dữ liệu theo cách này.



# AN NINH MẠNG (CYBERSECURITY)

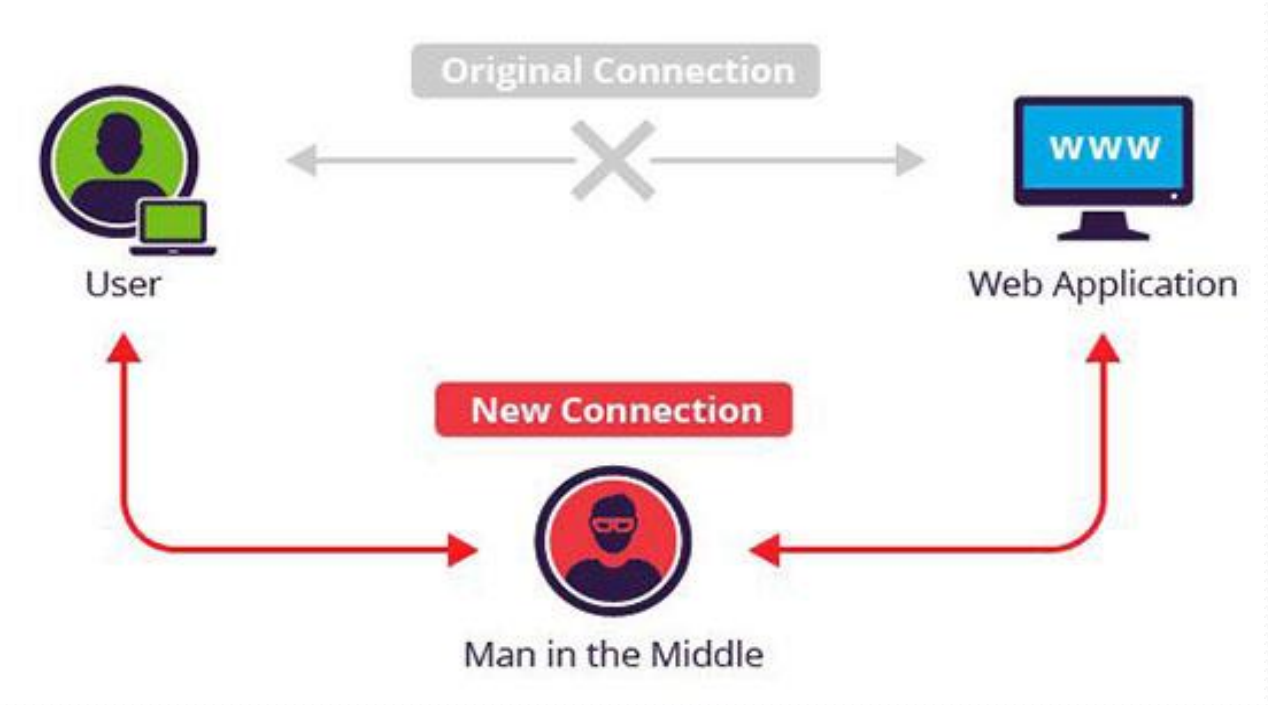
**4. Những phương pháp có thể đe dọa đến an ninh mạng**

**4.3. Tấn công giả mạo:** Tấn công giả mạo là phương thức tội phạm gửi email giả mạo các công ty uy tín yêu cầu khách hàng cung cấp các thông tin nhạy cảm. Tấn công giả mạo thường dùng để lừa lấy những dữ liệu thẻ ngân hàng hoặc các thông tin cá nhân khác.

# AN NINH MẠNG (CYBERSECURITY)

**4. Những phương pháp có thể đe dọa đến an ninh mạng:**

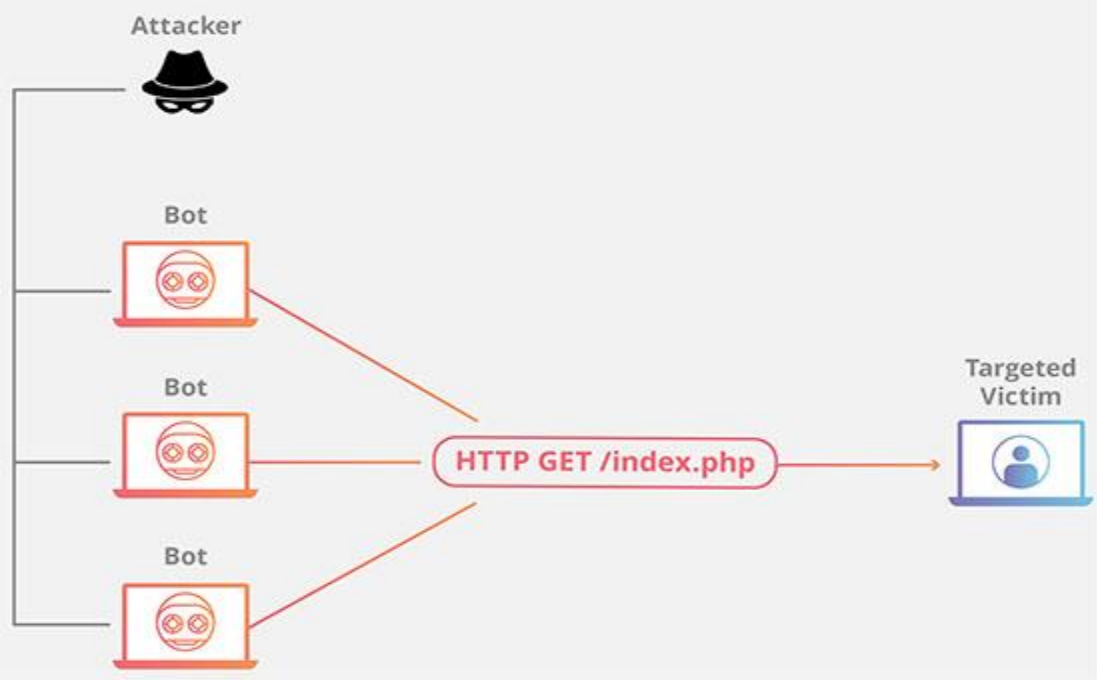
**4.4. Tấn công xen giữa:** là các tội phạm ngăn chặn giao tiếp, truyền tin giữa hai cá nhân nhằm mục đích ăn cắp dữ liệu. Ví dụ, trong một mạng WiFi không bảo mật, kẻ tấn công có thể ăn cắp các dữ liệu khi nó đang được truyền giữa hai thiết bị trong mạng đó.



# AN NINH MẠNG (CYBERSECURITY)

**4. Những phương pháp có thể đe dọa đến an ninh mạng:**

**4.5. Tấn công từ chối dịch vụ:** ngăn chặn một hệ thống máy tính thực hiện các yêu cầu hợp pháp bằng cách áp đảo các mạng và máy chủ có lưu lượng truy cập. Điều này làm cho hệ thống không thể sử dụng được, ngăn chặn một tổ chức thực hiện các chức năng quan trọng.



# AN NINH MẠNG (CYBERSECURITY)

**5. Bảo vệ người dùng cuối**

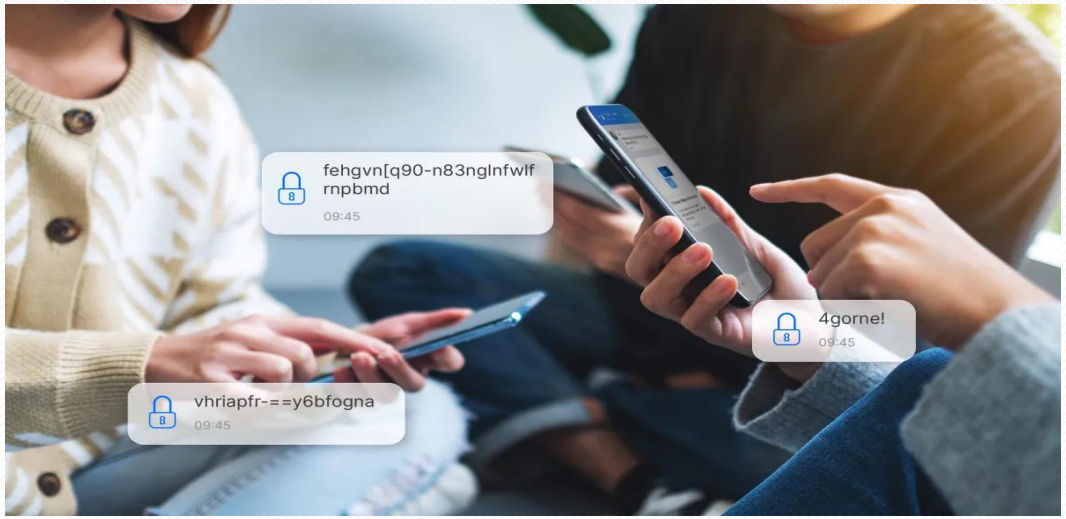
**5.1. Khái niệm:** Bảo vệ người dùng cuối hay bảo mật điểm cuối là một khía cạnh quan trọng của an ninh mạng. Sau tất cả, đe dọa an ninh mạng chỉ có thể xảy ra nếu một cá nhân (người dùng cuối) vô tình tải phần mềm độc hại hoặc các dạng mã độc khác xuống thiết bị của mình.

# AN NINH MẠNG (CYBERSECURITY)

**5. Bảo vệ người dùng cuối**

**5.2. Các phương pháp bảo vệ**

- Đầu tiên, an ninh mạng dựa vào các giao thức mã hóa để mã hóa email, file và các dữ liệu quan trọng khác. Nó không chỉ bảo vệ thông tin trong quá trình truyền tải mà còn ngăn chặn tình trạng bị mất hoặc đánh cắp.
- Thêm vào đó, những phần mềm bảo vệ người dùng thường xuyên quét máy để tìm những mã độc, cô lập các mã đó và xóa chúng khỏi hệ thống. Những chương trình này còn có thể nhận biết và loại bỏ những mã độc ẩn trong Master Boot Record và được thiết kế để mã hóa hoặc xóa dữ liệu khỏi ổ cứng máy tính.



# AN NINH MẠNG (CYBERSECURITY)

**5. Bảo vệ người dùng cuối**

**5.2. Các phương pháp bảo vệ**

- Các giao thức bảo mật điện tử tập trung vào việc phát hiện các phần mềm độc hại đang hoạt động. Chúng phân tích hành vi và tính tự phát của một chương trình và điều khiển nó chống lại virus hoặc Trojans, khiến chúng biến dạng sau mỗi lần tấn công. Các phần mềm an ninh còn có thể giới hạn những chương trình tiềm tàng mã độc, đẩy chúng vào một bong bóng ảo tách biệt với mạng của người dùng để phân tích hành vi và phát hiện mã độc nhanh hơn.
- Không những vậy, các chương trình an ninh còn phát triển thêm những hàng rào an ninh mạng chuyên nghiệp mới, giúp nhận biết các mối đe dọa mới xâm nhập và tạo ra nhiều cách thức hơn để chống lại chúng. Để có được một hệ thống mạng an toàn nhất, người dùng phải được đào tạo về cách thức sử dụng chúng. Quan trọng hơn, cập nhật các phiên bản ứng dụng mới thường xuyên là cách người dùng bảo vệ chính bản thân mình khỏi những mối đe dọa an ninh mạng mới nhất.

# AN NINH MẠNG (CYBERSECURITY)

**6. Phương pháp bảo vệ tổ chức và cá nhân khỏi tấn công mạng**

- **Cập nhật ứng dụng và hệ điều hành thường xuyên**: việc làm này giúp bạn tránh được những lỗ hổng an ninh mới nhất.
- **Sử dụng phần mềm anti-virus**: giải pháp an ninh này sẽ giúp bạn phát hiện và tiêu diệt mối đe dọa nhanh chóng. Nhưng hãy nhớ cập nhật phiên bản mới thường xuyên để luôn được bảo vệ ở mức cao nhất nhé.
- **Sử dụng mật khẩu mạnh**: hãy chắc chắn rằng mật khẩu của bạn không thể dễ dàng bị đoán ra.
- **Đừng mở email từ những nguồn không xác định**: đây là con đường dễ nhất để các phần mềm độc hại xâm nhập vào máy bạn.
- **Đừng click vào bất cứ đường link từ email hoặc trang web không rõ nguồn gốc**: lí do cũng tương tự như trên.
- **Tránh sử dụng WiFi không có bảo mật ở nơi công cộng**: một hệ thống mạng không có bảo mật sẽ rất dễ dàng bị tấn công xen giữa.

# TRÍ TUỆ NHÂN TẠO VÀ AN NINH MẠNG (CYBERSECURITY)

## 1. Sự trỗi dậy của trí tuệ nhân tạo

- Báo cáo Tin tức An ninh mạng thường niên của Cisco cho thấy, hơn 30% giám đốc về an ninh thông tin đã áp dụng AI như một cách để cải thiện hiệu quả tổng thể của chiến lược an ninh mạng. Các nhà lãnh đạo báo cáo rằng, hiện tại, họ hoàn toàn phụ thuộc vào AI để bảo vệ mạng và dữ liệu nhạy cảm của họ.
- Khi mã độc hại trở nên tiên tiến hơn, chúng đã học cách che giấu bản thân tốt hơn. Các mã độc hại mới có thể tự thay đổi mã, khiến công nghệ bảo mật cũ gần như không thể phát hiện ra chúng. Tuy nhiên, các giải pháp an ninh mạng dựa trên AI có thể xác định các hành vi độc hại trong lưu lượng mạng và các tệp, các trang web được đưa vào mạng.

# TRÍ TUỆ NHÂN TẠO VÀ AN NINH MẠNG (CYBERSECURITY)

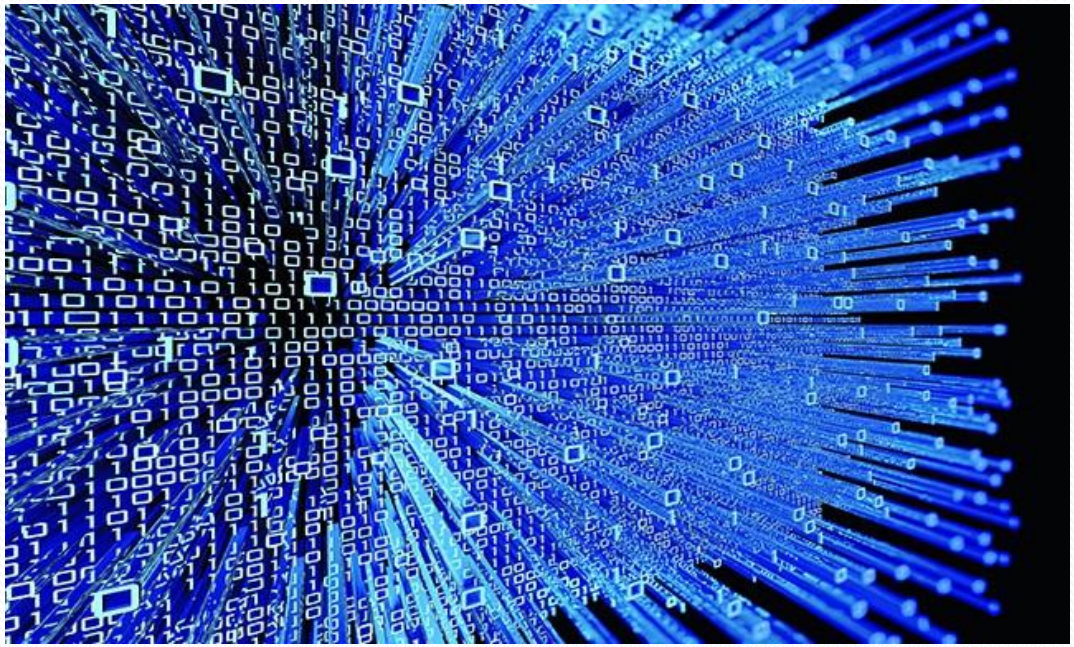
## 1. Sự trỗi dậy của trí tuệ nhân tạo

- Thông qua học máy, AI trở nên thông minh hơn, học cách xác định được các mẫu hành vi phức tạp hơn. Học máy có thể được sử dụng để điều chỉnh giải pháp dựa trên AI cho phù hợp với môi trường cụ thể và có thể được sử dụng để xác định các mối đe dọa phức tạp hơn. Tuy nhiên, nó vẫn cần sự hướng dẫn của con người và điều chỉnh.
- Các chuyên gia bảo mật không phải là những người duy nhất sử dụng AI, những kẻ tấn công cũng đã ứng dụng công nghệ này rất hiệu quả. Vấn đề này đã leo thang thành một cuộc chạy đua vũ trang giữa hai bên, giữa các chương trình độc hại và các giải pháp bảo mật ngày càng trở nên thông minh hơn.

# TRÍ TUỆ NHÂN TẠO VÀ AN NINH MẠNG (CYBERSECURITY)

## 2. Ưu điểm của trí tuệ nhân tạo trong an ninh mạng

- **AI có thể xử lý khối lượng dữ liệu lớn:** AI tự động hóa quá trình phát hiện các mối đe dọa tiên tiến. Nó có thể phân tích khối lượng rất lớn hoạt động diễn ra trên mạng của công ty với khối lượng lớn tập tin, tệp và trang web được nhân viên truy cập trong một thời gian rất ngắn. Mặc dù, AI không chính xác 100% trong việc phát hiện các mối đe dọa, nhưng nó có thể xác định phần lớn các hoạt động và mẫu nào là an toàn, cho phép con người tập trung vào một số lượng tương đối nhỏ phần còn lại đáng ngờ, có khả năng độc hại.



# TRÍ TUỆ NHÂN TẠO VÀ AN NINH MẠNG (CYBERSECURITY)

## 2. Ưu điểm của trí tuệ nhân tạo trong an ninh mạng

- **AI có thể học hỏi theo thời gian:** AI có thể xác định các cuộc tấn công độc hại dựa trên hành vi của các ứng dụng và hành vi của mạng nói chung. Theo thời gian, các giải pháp an ninh mạng sử dụng AI có thể tìm hiểu về lưu lượng truy cập thường xuyên và các hành vi của mạng và có thể phát hiện ra những bất thường so với chuẩn mực.
- **AI có thể xác định các mối đe dọa chưa biết:** AI có thể được sử dụng để tích lũy và tổng hợp thông tin về các mối đe dọa lan truyền hiện tại, tạo cơ sở dữ liệu thông minh, phân loại rủi ro và ứng phó với các mối đe doạ trong tương lai.

# TRÍ TUỆ NHÂN TẠO VÀ AN NINH MẠNG (CYBERSECURITY)

## 3. Giới hạn của trí tuệ nhân tạo với an ninh mạng

**Các mối đe dọa mạng không ngừng phát triển:** Những tội phạm mạng luôn phát triển và có nguồn lực hầu như không giới hạn. Khi các mối đe dọa mới xuất hiện, các giải pháp bảo mật sử dụng AI phải được đào tạo lại để theo kịp.

**Tội phạm mạng cũng sử dụng AI:** Tội phạm mạng có thể có được các giải pháp an ninh mạng sử dụng AI và kiểm tra các mã độc do họ viết ra với các giải pháp này. Do đó, về mặt lý thuyết, họ có thể tạo ra một chủng phần mềm độc hại có tích hợp AI. Họ cũng sử dụng máy học để hiểu hệ thống bảo mật dựa trên AI đang tìm kiếm những gì, sau đó có thể ngụy trang cuộc tấn công của họ hoặc biến đổi các mẫu để cuộc tấn công của họ có vẻ lành tính.

**Tính chính xác vẫn bị giới hạn:** Hệ thống AI vẫn chưa đủ tiên tiến để có thể phân biệt chính xác 100% hoạt động độc hại và lành tính. Để bảo vệ mạng cũng như các ứng dụng và dữ liệu trên mạng, hầu hết các giải pháp an ninh mạng, bao gồm cả các giải pháp dựa trên AI đều phải thận trọng. Khi gán nhãn bất thường cho quá nhiều hành vi bình thường sẽ khiến các chuyên gia phân tích bị tăng cường lượng công việc cần xử lý và có thể bỏ qua các cuộc tấn công thực sự.

# KẾT LUẬN

- Trong khi ứng dụng AI trong nhiều lĩnh vực là xu hướng tất yếu vì mang lại hiệu quả cao cho công việc, thì an ninh mạng là lĩnh vực nhận được sự quan tâm đặc biệt.
- Giữ an toàn cho mạng và hệ thống không phải là nhiệm vụ đơn giản. Nhưng hiện tại đã có sự hỗ trợ từ AI để củng cố an ninh mạng trong hệ thống.
- Những lợi ích đi kèm với việc sử dụng AI trong an ninh mạng là không thể so sánh được, từ việc quản lý khối lượng lớn dữ liệu về mối đe dọa đến phát hiện và phản hồi nhanh chóng. Điều quan trọng nhất là công nghệ về AI sẽ ngày càng phát triển và đến một lúc sẽ đóng một vài trò chính trong an ninh mạng./.

# Thank you very much!

If you need any information about content in my presentation, please fell free to contact me:

Nguyen Xuan Thuy. Tel: 84.913.525.444
Email: Thuynx@vea.gov.vn