

BẢO ĐẢM AN NINH QUỐC GIA TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

NGUYỄN VĂN THÀNH*
LỤC ANH TUẤN**

Cuộc cách mạng công nghiệp 4.0 đã và đang diễn ra một cách nhanh chóng chưa từng có với đặc trưng là điều khiển hệ thống và robot; các hệ thống liên kết thế giới thực và thế giới ảo do sự đột phá của khoa học - công nghệ dựa trên nền tảng công nghệ số tích hợp công nghệ "thông minh" để tối ưu hóa quy trình, phương thức sản xuất. Điểm "đòn bẩy" là trí tuệ nhân tạo (AI); công nghệ in 3D, công nghệ sinh học, công nghệ vật liệu mới, công nghệ tự động hóa, robot, internet kết nối vạn vật (IoT) và Internet các dịch vụ (IoS) đang dần trở thành những công cụ sản xuất quan trọng trong nhiều ngành, lĩnh vực. Bên cạnh mặt tích cực, công nghệ 4.0 cũng đang đặt ra không ít những thách thức, đặc biệt là trong lĩnh vực bảo đảm an ninh quốc gia. Do đó, rất cần có những giải pháp phù hợp trong bối cảnh số hóa hiện nay.

Từ khóa: An ninh quốc gia, chuyển đổi số, cách mạng công nghiệp; bảo đảm.

The Industrial Revolution 4.0 has been progressing at an unprecedented pace, marked by advancements in system controls and robotics, as well as the integration of physical and virtual worlds. It is driven by breakthroughs in science and technology, particularly in digital technologies, which incorporate "smart" technologies to optimize processes and production methods. Key technologies, known as "leverage points," include artificial intelligence (AI), 3D printing, biotechnology, new materials, automation, robotics, the Internet of Things (IoT), and the Internet of Services (IoS). These technologies are increasingly becoming essential tools for production across various industries and sectors. While Industry 4.0 has many positive aspects, it also poses significant challenges, particularly concerning national security. Therefore, it is essential to implement effective solutions in the current context of digitalization.

Keywords: National security; digital transformation; industrial revolution; ensure.

NGÀY NHẬN: 11/11/2024

NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 15/12/2024

NGÀY DUYỆT: 10/01/2025

DOI: <https://doi.org/10.59394/qlnn.348.2025.1057>

1. Đặt vấn đề

Theo TS. Truchard, cách mạng công nghiệp 4.0 mở ra thời đại mới, vượt qua phạm vi của công nghệ thông tin và điện tử, được thúc đẩy bởi các hệ thống tích hợp cả dữ liệu kỹ thuật số và dữ liệu tương tự trên môi

trường tính toán và vật lý; thay đổi ngành công nghiệp theo một số cách thức chính: dữ

* *Thượng tướng, PGS, TS. Hội đồng Lý luận Trung ương*

** *TS. Hội đồng Lý luận Trung ương*

liệu tương tự lớn (big analog data), thiết bị kích thước nhỏ hơn nhưng hiệu suất cao hơn, không còn khoảng cách địa lý và việc giáo dục dễ dàng hơn¹.

Không gian mạng đã trở thành môi trường thứ Năm với sự ra đời của chiến tranh mạng, tác động sâu sắc đến quốc phòng, an ninh của mọi quốc gia². Nội hàm khái niệm an ninh quốc gia được mở rộng, không chỉ còn giới hạn ở trên đất liền mà đã mở rộng xuống ngầm, trên không, trên biển và trên không gian mạng. Công nghệ thông tin tạo ra những thách thức lớn đối với bảo đảm an ninh quốc gia, đặc biệt là vấn đề tội phạm công nghệ cao, an ninh thông tin, an ninh mạng, trong khi Việt Nam chưa tự chủ hoàn toàn về công nghệ, gây nguy cơ mất chủ quyền an ninh thông tin, ở một góc độ nào đó có thể tạo ra hệ lụy rất nguy hiểm.

Một ví dụ nổi bật là sự phát triển nhanh chóng của trí tuệ nhân tạo (AI) thời gian qua đem lại những thay đổi to lớn đối với đời sống kinh tế, chính trị, xã hội trên thế giới. Tuy nhiên, AI cũng đặt ra nhiều thách thức, như: sự gia tăng của các cuộc tấn công mạng thông qua AI (gây thiệt hại kinh tế thế giới khoảng 8.000 tỷ USD năm 2023, ảnh hưởng đến 353 triệu người; dự kiến con số thiệt hại kinh tế sẽ là 9.500 tỷ USD năm 2024)³; nguy cơ các đối tượng khủng bố lợi dụng AI để thực hiện các mục đích xấu, như: gửi email độc hại, phát tán thông tin sai lệch, thu hút người ủng hộ, lên kế hoạch tấn công khủng bố; hay việc các đối tượng lợi dụng công nghệ deepfake để tạo ra ảnh khuôn mặt giả nhằm vào phụ nữ và trẻ em tại Mỹ, Hàn Quốc...⁴. Thực tế này minh chứng cho tác động nhiều mặt của cách mạng công nghiệp 4.0. Các quốc gia đều phải tư duy lại cách thức quản trị, phát triển theo hướng tận dụng mặt tích cực của khoa học - công nghệ để phát triển, tăng tính cạnh tranh quốc gia, đồng thời giảm thiểu tác động tiêu cực mà cách mạng công nghiệp 4.0 có thể mang lại (*xem hình 1 cuối bài*).

Tuy nhiên, cùng với những lợi ích to lớn về công nghệ thông tin thì cũng đang phải đối mặt với rất nhiều nguy cơ và thách thức trước những cuộc tấn công mạng không còn đơn thuần là khai thác lỗ hổng, phá hoại thông thường mà mục tiêu rõ rệt là nhắm tới các tổ chức tài chính, hệ thống máy tính của ngân hàng, hệ thống thương mại điện tử, chính phủ điện tử...

2. Chuyển đổi số là một cuộc cách mạng

Đảng và Nhà nước ta rất coi trọng công tác chuyển đổi số, xác định là một trong những nhiệm vụ trọng tâm hàng đầu giúp đất nước tận dụng được những cơ hội của cách mạng công nghiệp 4.0, tạo bứt phá, thu hẹp khoảng cách với các nước phát triển, vượt ra khỏi bẫy thu nhập trung bình, hướng tới một nền kinh tế phát triển bền vững, mau chóng tiến kịp với các nước phát triển trên thế giới.

Bộ Chính trị ban hành Nghị quyết số 36-NQ/TW ngày 01/7/2014 về đẩy mạnh ứng dụng, phát triển công nghệ thông tin đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế; Nghị quyết số 52-NQ/TW ngày 27/9/2019 về một số chủ trương, chính sách chủ động tham gia cuộc cách mạng công nghiệp 4.0. Trong đó, thẳng thắn đánh giá: “Quá trình chuyển đổi số quốc gia còn chậm, thiếu chủ động do hạ tầng phục vụ quá trình chuyển đổi số còn nhiều hạn chế; nhiều doanh nghiệp còn bị động, năng lực tiếp cận, ứng dụng, phát triển công nghệ hiện đại còn thấp”; đồng thời, đặt ra một số mục tiêu cụ thể đến năm 2025, định hướng đến năm 2030 và tầm nhìn đến năm 2045.

Thủ tướng Chính phủ ban hành Quyết định số 749/QĐ-TTg ngày 03/6/2020 phê duyệt “Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030” với mục tiêu đưa Việt Nam vào nhóm 50 nước dẫn đầu về chính phủ điện tử (EGDI)⁵. Chương trình chuyển đổi số quốc gia xác định: nhận thức đóng vai trò quyết định

trong chuyển đổi số; người dân là trung tâm của chuyển đổi số; thể chế và công nghệ là động lực của chuyển đổi số; phát triển nền tảng số là giải pháp đột phá để thúc đẩy chuyển đổi số nhanh hơn, giảm chi phí, tăng hiệu quả; bảo đảm an toàn, an ninh mạng là then chốt để chuyển đổi số thành công và bền vững, đồng thời là phần xuyên suốt, không thể tách rời của chuyển đổi số và sự vào cuộc của cả hệ thống chính trị, hành động đồng bộ ở các cấp, sự tham gia của toàn dân là yếu tố bảo đảm sự thành công của chuyển đổi số. Xác định mục tiêu cơ bản đến năm 2025, định hướng đến năm 2030 trên các tiêu chí: (1) Phát triển Chính phủ số, nâng cao hiệu quả, hiệu lực hoạt động; (2) Phát triển kinh tế số, nâng cao năng lực cạnh tranh của nền kinh tế; (3) Phát triển xã hội số, thu hẹp khoảng cách số.

Tổng Bí thư Tô Lâm đã nhấn mạnh về sự cần thiết phải tiến hành cuộc cách mạng chuyển đổi số để điều chỉnh quan hệ sản xuất, tạo động lực mới cho phát triển. Chuyển đổi số không đơn thuần là việc ứng dụng công nghệ số vào các hoạt động kinh tế - xã hội mà còn là quá trình xác lập một phương thức sản xuất mới tiên tiến, hiện đại - “phương thức sản xuất số”, trong đó đặc trưng của lực lượng sản xuất là sự kết hợp hài hòa giữa con người và trí tuệ nhân tạo; dữ liệu trở thành một tài nguyên, trở thành tư liệu sản xuất quan trọng; đồng thời, quan hệ sản xuất cũng có những biến đổi sâu sắc, đặc biệt là trong hình thức sở hữu và phân phối tư liệu sản xuất số⁶. Phương châm đặt ra là: thực hiện cách mạng chuyển đổi số với những cải cách mạnh mẽ, toàn diện để điều chỉnh quan hệ sản xuất, tạo động lực mới cho phát triển, tranh thủ tối đa thời cơ, thuận lợi do cách mạng công nghiệp 4.0 đem lại, đưa đất nước đi tắt, đón đầu phát triển vượt bậc⁷.

3. Tình hình tội phạm lợi dụng tiến bộ khoa học - công nghệ hiện nay

Thực tiễn cho thấy, không gian mạng và một số loại hình dịch vụ, ứng dụng công nghệ

thông tin đang là công cụ để các thế lực thù địch, tội phạm lợi dụng thực hiện hoạt động⁸. Số lượng các vụ tấn công mạng diễn ra ngày càng nhiều trên thế giới, gây ra thiệt hại nghiêm trọng, đặc biệt là trong bối cảnh đại dịch Covid-19 khi các chính phủ và doanh nghiệp phải chuyển sang trạng thái làm việc từ xa. Các cuộc tấn công bằng phần mềm độc hại đã tăng từng năm. Ví dụ tăng 358% năm 2020 so với năm 2019; tăng 125% năm 2021 so với năm 2020⁹. Số vụ tấn công mạng năm 2023 là 2.365 vụ với hơn 343 triệu nạn nhân. Trong các vụ tấn công bằng phần mềm độc hại, tấn công qua email là dạng phổ biến nhất, chiếm khoảng 35% số vụ tấn công¹⁰.

Tình hình tội phạm sử dụng công nghệ cao tại Việt Nam thời gian qua diễn biến ngày càng phức tạp.

Thứ nhất, không gian mạng và một số loại hình dịch vụ, ứng dụng công nghệ thông tin đang bị các thế lực thù địch, phản động sử dụng để thực hiện âm mưu tiến hành “cách mạng màu”, “cách mạng đường phố”, “diễn biến hòa bình” với mục tiêu thâm độc xóa bỏ chế độ chính trị ở nước ta. Theo thống kê của Bộ Công an, trong gần 10 năm qua, các thế lực thù địch, phần tử xấu đã, đang sử dụng 8.784 web, blog có tên miền nước ngoài; 381 web, blog có tên miền trong nước thường xuyên đăng tải thông tin xấu, độc chống phá Đảng, Nhà nước Việt Nam; đã phát hiện 279 vụ sử dụng internet xâm phạm an ninh quốc gia, đấu tranh với hơn 200 đối tượng; xử lý 140 đối tượng. Đáng chú ý, trong đó có 219 vụ kích động biểu tình trên không gian mạng; 138 hội, nhóm trá hình hoạt động trên không gian mạng; 45.498 lượt cổng thông tin, trang tin điện tử có tên miền “.vn” bị tấn công, trong đó có 2.113 lượt tấn công các cổng thông tin, trang tin điện tử của cơ quan Đảng, Nhà nước gây ra những hậu quả nghiêm trọng¹¹.

Thứ hai, ngày càng xuất hiện nhiều cuộc tấn công mạng, lừa đảo qua không gian mạng với quy mô lớn, cường độ cao, gia tăng

về tính chất nghiêm trọng, mức độ nguy hiểm, đe dọa trực tiếp đến an ninh quốc gia và trật tự, an toàn xã hội. Theo báo cáo gần đây của Microsoft, tỷ lệ tấn công nhằm vào Việt Nam sử dụng phần mềm độc hại ransomware cao nhất ở châu Á - Thái Bình Dương, là một trong ba quốc gia trong khu vực bị ảnh hưởng nhiều nhất của các cuộc tấn công phần mềm độc hại (sau Indonesia và Sri Lanka) và đứng thứ sáu trên thế giới về số lượt tải mã độc không chủ ý¹². Khủng bố mạng nổi lên như một thách thức đe dọa nghiêm trọng tới an ninh quốc gia.

Hoạt động phạm tội trên không gian mạng ngày càng gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về kinh tế, ảnh hưởng đến tư tưởng, văn hóa - xã hội. Theo số liệu từ Cục An toàn thông tin (Bộ Thông tin và Truyền thông), trong 11 tháng đầu năm 2022, đã có tới 11.213 cuộc tấn công mạng hướng vào Việt Nam, tăng 44,2% so với cùng kỳ năm 2021. Trong đó, có 3.930 cuộc tấn công giả mạo (phishing), 1.524 cuộc tấn công thay đổi nội dung (deface), 5.759 cuộc tấn công phần mềm độc hại (malware). Trong năm 2022, tình trạng giả mạo thương hiệu gia tăng đột biến (chiếm 72,6% số vụ lừa đảo trên mạng được ghi nhận); ngoài ra, còn có giả mạo chiếm đoạt tài sản trực tuyến (chiếm 11,4%), lừa đảo trúng thưởng, việc làm online, ứng dụng cho vay... (chiếm 16%)¹³.

Chỉ trong 9 tháng đầu năm 2024, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an) đã tổ chức đấu tranh, triệt phá, phối hợp với cơ quan điều tra các cấp khởi tố 14 vụ án, với 75 bị can liên quan các đường dây lừa đảo chiếm đoạt tài sản qua mạng, tổ chức đánh bạc, đánh bạc, mua bán ma túy, chất cấm qua mạng. Đặc biệt đáng lo ngại là tình trạng lây nhiễm virus và xuất hiện phần mềm gián điệp gây nguy cơ mất an ninh, an toàn hệ thống thông tin mạng¹⁴.

Thứ ba, việc có nhiều thiết bị kết nối internet, đặc biệt là sự phát triển nhanh chóng của mạng lưới IoT là nguy cơ dẫn đến lộ lọt bí mật nhà nước và các thông tin cá nhân, quyền riêng tư, các đối tượng triệt để lợi dụng các kẽ hở trong bảo mật thông tin, bảo mật tài liệu để thực hiện các cuộc tấn công quy mô lớn nhằm đánh cắp thông tin và sử dụng để can thiệp hoạt động chính trị hoặc thực hiện các hành vi vi phạm pháp luật. Theo lãnh đạo Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao (Bộ Công an), trong năm 2021, cơ quan chức năng phát hiện 30 vụ lộ, mất bí mật nhà nước với 202 đầu tài liệu¹⁵.

Thứ tư, công tác quản lý, giáo dục chính trị tư tưởng cho cán bộ, chiến sĩ gặp nhiều khó khăn trong bối cảnh bùng nổ của công nghệ, các thông tin thất thiệt trên mạng internet gây nhiều loạn, hoang mang trong dư luận. Việc quản lý cán bộ, chiến sĩ tham gia các trang mạng xã hội, như: Facebook, Tik Tok, Instagram, Twitter...; việc sử dụng các thiết bị công nghệ hiện đại chưa được thực hiện đầy đủ, chặt chẽ, dẫn đến nguy cơ lộ lọt thông tin cá nhân, bí mật nhà nước liên quan đến ngành Công an ngày càng gia tăng.

4. Yêu cầu đối với công tác bảo đảm an ninh quốc gia trong bối cảnh đẩy mạnh chuyển đổi số tại Việt Nam

Đại hội đại biểu toàn quốc lần thứ XIII của Đảng xác định khoa học - công nghệ và đổi mới sáng tạo là một trong những khâu đột phá chiến lược quan trọng để xây dựng và phát triển Tổ quốc Việt Nam xã hội chủ nghĩa. Nghị quyết của Đại hội đưa ra mục tiêu cụ thể phát triển đất nước từ nay đến năm 2045; cụ thể: đến năm 2025, kỷ niệm 50 năm giải phóng hoàn toàn miền Nam, thống nhất đất nước, là nước đang phát triển, có công nghiệp theo hướng hiện đại, vượt qua mức thu nhập trung bình thấp. Đến năm 2030, kỷ niệm 100 năm thành lập Đảng là nước đang phát triển, có công nghiệp hiện

đại, thu nhập trung bình cao. Đến năm 2045, kỷ niệm 100 năm thành lập nước: trở thành nước phát triển, thu nhập cao. Trong đó, đặc biệt cần thiết phải tiến hành chuyển đổi số, “quá trình chuyển đổi số cần được thực hiện toàn diện, đồng bộ, có tính đến mối quan hệ biện chứng giữa cơ sở hạ tầng và kiến trúc thượng tầng nhằm xây dựng nền kinh tế thị trường định hướng xã hội chủ nghĩa, vừa phát huy sức mạnh của lực lượng sản xuất hiện đại, vừa bảo đảm bản chất tốt đẹp của chế độ xã hội chủ nghĩa, phù hợp với điều kiện cụ thể của Việt Nam trong thời đại mới”¹⁶; đồng thời, quán triệt việc đẩy mạnh chuyển đổi số phải gắn liền với bảo đảm an ninh để Việt Nam bứt phá trong kỷ nguyên mới.

Để đạt được mục tiêu này, khuyến nghị các nhóm giải pháp sau:

Một là, chủ động quán triệt, triển khai thực hiện có hiệu quả các quan điểm, chủ trương của Đảng, chính sách, pháp luật của Nhà nước về chuyển đổi số, phát triển khoa học - công nghệ và xây dựng lực lượng vũ trang nhân dân trong bối cảnh tình hình mới, nhất là những mục tiêu, nhiệm vụ đã được xác định trong Nghị quyết Đại hội Đảng toàn quốc lần thứ XIII; Nghị quyết số 52-NQ/TW ngày 27/9/2019 của Bộ Chính trị về một số chủ trương, chính sách chủ động tham gia cuộc cách mạng công nghiệp 4.0; Chỉ thị số 16/CT-TTg ngày 04/5/2017 của Thủ tướng Chính phủ về việc tăng cường năng lực tiếp cận cuộc cách mạng công nghiệp 4.0; Nghị quyết số 12-NQ/TW về đẩy mạnh xây dựng lực lượng Công an nhân dân thật sự trong sạch, vững mạnh, chính quy, tinh nhuệ, hiện đại, đáp ứng yêu cầu, nhiệm vụ trong tình hình mới; Nghị quyết số 44-NQ/TW ngày 24/11/2023 của Hội nghị Trung ương 8 (khóa XIII) về Chiến lược bảo vệ Tổ quốc trong tình hình mới. Tiếp tục triển khai hiệu quả Đề án phát triển ứng dụng dữ liệu về dân cư, định danh và xác thực điện tử phục vụ chuyển đổi số quốc gia giai đoạn

2022 - 2025, tầm nhìn đến năm 2030 của Chính phủ (Đề án 06).

Hai là, cấp ủy, lãnh đạo các cấp cần nâng cao hơn nữa nhận thức của cán bộ, đảng viên về tác động và những vấn đề đặt ra trong việc đẩy mạnh chuyển đổi số quốc gia và cách mạng công nghiệp 4.0 mang lại, đặc biệt là tác động đối với an ninh quốc gia để cán bộ, công chức tự ý thức về sự cần thiết có khả năng làm chủ các thành tựu khoa học - công nghệ; nắm được âm mưu, thủ đoạn chống phá của các thế lực thù địch, các loại tội phạm và vi phạm pháp luật khác trong bối cảnh chuyển đổi số quốc gia, cách mạng công nghiệp 4.0 để tự bảo vệ mình, bảo vệ bí mật nhà nước trong môi trường không gian mạng.

Ba là, các lực lượng chuyên trách của Bộ Công an, Bộ Quốc phòng... cần dự báo được những nguy cơ, thách thức đối với công tác bảo đảm an ninh quốc gia trong bối cảnh đẩy mạnh chuyển đổi số và đề xuất biện pháp ngăn chặn, đấu tranh hiệu quả, phù hợp. Tận dụng tối đa những thành quả của cuộc cách mạng công nghiệp 4.0 trong triển khai sắp xếp tổ chức bộ máy lực lượng chuyên trách bảo đảm an ninh quốc gia, bố trí cán bộ tinh gọn, hiệu quả. Phát huy tối đa lợi thế của mạng internet, tăng cường cung cấp, cập nhật thường xuyên các thông tin, quan điểm đúng đắn của Đảng, Nhà nước trên các website, cổng thông tin điện tử nhằm nâng cao nhận thức, ý thức chính trị của người dân, đấu tranh chống lại các quan điểm, luận điệu sai trái của các thế lực thù địch.

Bốn là, đẩy mạnh hợp tác quốc tế, tăng cường hợp tác với các nước có trình độ cao về khoa học - công nghệ, tranh thủ tối đa mọi nguồn lực để phát triển khoa học - công nghiệp quốc phòng, an ninh lưỡng dụng, hiện đại; quan tâm đầu tư mua sắm nâng cấp hệ thống hạ tầng thông tin quốc gia.

Năm là, kiện toàn, nâng cao chất lượng đào tạo cán bộ chuyên trách bảo đảm an ninh quốc gia, đáp ứng các yêu cầu (như

trình độ cao về lý luận, nghiệp vụ, khoa học - công nghệ...) ngang tầm nhiệm vụ trong bối cảnh đẩy mạnh chuyển đổi số quốc gia và cách mạng công nghiệp 4.0

Chú thích:

1. *5 Ways Cyber-Physical Systems are Transforming Manufacturing*. <https://www.mddionline.com/equipment/5-ways-cyber-physical-systems-are-transforming-manufacturing>, ngày 14/02/2014.

2. Adib Farhadi, Ronald P. Sanders, and Anthony Masys, eds. *The Great Power Competition Volume 3: Cyberspace: The Fifth Domain*. Springer Nature, 2022.

3. *Tấn công mạng thông qua AI gây tổn thất kinh tế nghiêm trọng*. <https://thoibaotaichinhvietnam.vn>, ngày 31/5/2024.

4. *Giới chuyên gia lo ngại khủng bố lợi dụng trí tuệ nhân tạo*. <https://baotintuc.vn>, ngày 03/9/2024.

5. Chỉ số Phát triển Chính phủ điện tử (E-Government Development Index là chỉ số đánh giá tình hình Phát triển Chính phủ điện tử của các quốc gia thành viên Liên hiệp quốc; gồm các tiêu chí như: các mô hình phát triển trang web tại một quốc gia, việc quốc gia đang sử dụng công nghệ thông tin để thúc đẩy khả năng tiếp cận và hòa nhập của người dân... EGDI là thước đo tổng hợp của ba chiều quan trọng của chính

phủ điện tử, cụ thể là: cung cấp dịch vụ trực tuyến, kết nối viễn thông và năng lực con người. <https://publicadministration.un.org>

6, 16. *Toàn văn bài viết về chuyển đổi số của Tổng Bí thư, Chủ tịch nước Tô Lâm*. <https://tienphong.vn>, ngày 02/9/2024.

7. *Một số nội dung cơ bản về kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc; những định hướng chiến lược đưa đất nước bước vào kỷ nguyên mới, kỷ nguyên vươn mình của dân tộc*. <https://www.tapchiconsan.org.vn>, ngày 01/11/2024.

8. *Chủ quyền quốc gia trên không gian mạng - những yêu cầu đảm bảo các chỉ số an ninh - an toàn trong bối cảnh hiện nay*. <http://hdl.vn/vi>, ngày 09/12/2021.

9. *The latest 2023 cyber crime statistics (updated April 2023)*. <https://aag-it.com>

10. *Cybersecurity Stats: Facts and Figures You should Know*. <https://www.forbes.com>, ngày 28/8/2024.

11. *Tự chủ công nghệ và phát huy trách nhiệm của nhân dân*. <https://www.qdnd.vn>, ngày 11/12/2021.

12. *Microsoft Security Endpoint Threat Report 2019*. <https://news.microsoft.com>

13. *Số cuộc tấn công mạng hướng vào Việt Nam tăng hơn 44%*. <https://vtv.vn>, ngày 24/11/2022.

14, 15. *30 vụ lộ, mất bí mật nhà nước với hơn 200 đầu tài liệu trong năm 2021*. <https://vietnamnet.vn>, ngày 21/12/2021.

Hình 1. 15 lợi ích của công nghệ số

