

TRƯỜNG ĐẠI HỌC MỎ - ĐỊA CHẤT
KHOA GIÁO DỤC QUỐC PHÒNG



BÁO CÁO HỌC THUẬT

TÊN BÁO CÁO:

**NHỮNG ĐIỂM KHÁC BIỆT GIỮA DEEP WEB VÀ DARK WEB
VÀ CÁCH SỬ DỤNG CHÚNG SAO CHO CÓ HIỆU QUẢ**

Người thực hiện: HOÀNG XUÂN TRƯỜNG

Hà Nội, 06/2025

I. LÝ DO CHỌN BÁO CÁO

Internet thường được hình dung như một tầng băng trôi, với Surface Web (Web bề nổi) dễ dàng truy cập chỉ chiếm một phần nhỏ. Phần lớn còn lại là Deep Web, bao gồm các nội dung không được lập chỉ mục bởi các công cụ tìm kiếm tiêu chuẩn, và một phần nhỏ hơn trong đó là Dark Web, nổi tiếng với các hoạt động ẩn danh và thường liên quan đến các hành vi phi pháp. Thực tế trong thời gian vừa qua việc tổ chức giảng dạy và thực hành giảng dạy chuyên đề “An toàn thông tin và phòng, chống vi phạm pháp luật trên không gian mạng” trong môn học Công tác Quốc phòng và an ninh thời gian qua mặc dù Khoa và Bộ môn đã tổ chức giảng dạy theo đúng văn bản, chương trình đã được tập huấn, hướng dẫn. Song bên cạnh đó một số nội dung chưa được nghiên cứu làm rõ; tài liệu tham khảo, sách hướng dẫn còn hạn chế về mặt nội dung từ đó gây khó khăn cho công tác giảng dạy của giảng viên cũng như quá trình tự nghiên cứu của sinh viên.

Đúc kết qua quá trình giảng dạy tác giả đã tập trung tìm tòi, nghiên cứu và xây dựng ra bài viết này nhằm mục đích làm rõ sự khác biệt cơ bản giữa Deep Web và Dark Web, khám phá các công nghệ tạo điều kiện cho tính ẩn danh, đặc biệt là mạng Tor. Tác giả tập trung phân tích bản chất các hoạt động trên Dark Web, bao gồm cả các hoạt động hợp pháp và bất hợp pháp, dựa trên các nghiên cứu hiện có. Đồng thời, bài viết cũng giải quyết và bác bỏ một số lầm tưởng và thông tin sai lệch phổ biến về mức độ nguy hiểm và cấu trúc của Dark Web, như huyền thoại về các "tầng" của Dark Web hay những rủi ro bị thổi phồng khi truy cập. Mục tiêu là cung cấp một cái nhìn khách quan, dựa trên bằng chứng về các thành phần ẩn của Internet, khuyến khích sự hiểu biết đúng đắn và cách tiếp cận thông tin có chọn lọc hơn từ người dùng.

Xuất phát từ những vấn đề nêu trên, tác giả đề xuất nội dung học thuật ***"Những điểm khác biệt giữa Deep Web và Dark Web và cách sử dụng chúng sao cho hiệu quả"*** làm Báo cáo học thuật của Bộ môn học kỳ II năm học 2024 - 2025.

II. MỤC TIÊU NGHIÊN CỨU

Dựa trên các nghiên cứu khoa học, sẽ làm rõ định nghĩa, sự khác biệt giữa Deep Web và Dark Web, những nguy cơ tiềm ẩn cũng như một số khía cạnh sử

dụng cần được nhìn nhận một cách thận trọng và có hiểu biết. Thông qua học thuật tác giả, mong muốn cùng tìm hiểu đầy đủ hơn và sâu hơn về chúng để vận dụng vào quá trình giảng dạy chuyên đề ***“An toàn thông tin và phòng, chống vi phạm pháp luật trên không gian mạng”***.

III. ĐỐI TƯỢNG NGHIÊN CỨU

- Deep Web và Dark Web và các hành vi vi phạm pháp luật trên không gian mạng
- Những nguy cơ tiềm ẩn cũng như một số khía cạnh sử dụng cần được nhìn nhận một cách thận trọng và có hiểu biết.

IV. PHẠM VI NGHIÊN CỨU

- Giảng viên trong Khoa Giáo dục quốc phòng.
- Chuyên đề ***“An toàn thông tin và phòng, chống vi phạm pháp luật trên không gian mạng”***
- Sinh viên toàn trường khi tham gia học môn học Giáo dục Quốc phòng và an ninh.

NỘI DUNG

1. Định nghĩa Deep Web và Dark Web

Trước hết, cần phải khẳng định rằng Deep Web và Dark Web không phải là một. Để hiểu rõ, chúng ta có thể hình dung Internet như một tầng băng trôi:

- **Surface Web (Web bề nổi):** Đây là phần nổi của tầng băng, bao gồm tất cả các trang web có thể được truy cập thông qua các công cụ tìm kiếm thông thường như Google, Bing, DuckDuckGo. Các trang web này được lập chỉ mục (indexed) bởi các máy tìm kiếm. Ước tính, Surface Web chỉ chiếm một phần rất nhỏ, khoảng dưới 5% tổng lượng thông tin trên Internet.
- **Deep Web (Web chìm):** Đây là phần chìm của tầng băng, chiếm phần lớn nhất của Internet (ước tính khoảng 90-95%). Deep Web chứa đựng tất cả các nội dung trên mạng không được các công cụ tìm kiếm tiêu chuẩn lập chỉ mục. Điều này không đồng nghĩa với việc tất cả nội dung trong Deep Web đều là bất hợp pháp hay nguy hiểm. Thực tế, phần lớn Deep Web bao gồm các cơ sở dữ liệu, các mạng nội bộ của doanh nghiệp, trường học, chính phủ, các tài khoản trực tuyến (email, ngân hàng trực tuyến, lưu trữ đám mây), các tạp chí học thuật có trả phí, hồ sơ y tế, tài liệu pháp lý, và các nội dung yêu cầu đăng nhập hoặc xác thực để truy cập. Hầu hết chúng ta tương tác với Deep Web hàng ngày mà không hề hay biết.
- **Dark Web (Web tối):** Dark Web là một phần nhỏ, được ẩn đi một cách có chủ đích bên trong Deep Web. Nó được xây dựng trên các mạng được mã hóa đặc biệt gọi là "darknets" (ví dụ phổ biến nhất là Tor - The Onion Router, I2P - Invisible Internet Project, Freenet). Để truy cập Dark Web, người dùng cần các phần mềm, cấu hình hoặc ủy quyền truy cập đặc biệt. Đặc điểm chính của Dark Web là tính ẩn danh cao cho cả người dùng và nhà cung cấp nội dung. Chính vì tính ẩn danh này mà Dark Web thường bị gắn liền với các hoạt động bất hợp pháp.

2. Những điểm khác biệt cơ bản giữa Deep Web và Dark Web

Dựa trên các nghiên cứu, có thể chỉ ra những điểm khác biệt cốt lõi sau:

| Đặc điểm | Deep Web | Dark Web |
|-------------------|--|---|
| Khả năng truy cập | Có thể truy cập bằng trình duyệt thông thường nhưng cần URL trực tiếp hoặc thông tin đăng nhập. Không được lập chỉ mục bởi công cụ tìm kiếm. | Cần phần mềm chuyên dụng (ví dụ: Tor Browser) và thường là địa chỉ .onion hoặc tương tự. |
| Kích thước | Rất lớn, chiếm phần lớn Internet. | Nhỏ hơn nhiều so với Deep Web, chỉ là một phần của Deep Web. |
| Tính ẩn danh | Mức độ ẩn danh phụ thuộc vào từng trang cụ thể; nhiều trang yêu cầu xác thực danh tính. | Tính ẩn danh rất cao cho cả người dùng và máy chủ nhờ các lớp mã hóa và định tuyến phức tạp. |
| Nội dung chủ yếu | Cơ sở dữ liệu, tài khoản cá nhân, nội dung học thuật, báo cáo nội bộ, nội dung được bảo vệ bằng mật khẩu. | Diễn đàn ẩn danh, chợ đen trực tuyến (ma túy, vũ khí, dữ liệu bị đánh cắp), dịch vụ bất hợp pháp, nhưng cũng có các trang phục vụ tự do ngôn luận, bảo vệ nhà báo, nhà hoạt động. |
| Tính hợp pháp | Phần lớn là hợp pháp và cần thiết cho hoạt động hàng ngày của Internet. | Chứa đựng cả nội dung hợp pháp và một tỷ lệ đáng kể nội dung bất hợp pháp, nguy hiểm. |

3. Mức độ nguy hiểm và những quan niệm

Những mô tả về một "nơi đen tối nhất trên Internet" với vô vàn vấn đề nguy hiểm thường nhắm đến Dark Web, chứ không phải toàn bộ Deep Web.

Đối với Deep Web: Như đã đề cập, phần lớn Deep Web là hợp pháp và an toàn, chứa đựng thông tin cần thiết cho hoạt động của xã hội hiện đại. Nguy cơ chủ yếu khi tương tác với Deep Web thường liên quan đến việc bảo mật thông tin cá nhân

(ví dụ: lộ mật khẩu email, tài khoản ngân hàng). Tuy nhiên, đây là những rủi ro chung của việc sử dụng Internet, không phải đặc thù chỉ có ở Deep Web.

Đối với Dark Web: Dark Web, với tính ẩn danh cao, thực sự là nơi tiềm ẩn nhiều nguy cơ nghiêm trọng và là môi trường cho nhiều hoạt động bất hợp pháp như:

- **Buôn bán hàng cấm:** Ma túy, vũ khí, dữ liệu thẻ tín dụng bị đánh cắp, phần mềm độc hại, thông tin cá nhân bị rò rỉ.
- **Nội dung đồi trụy và bạo lực:** Bao gồm cả những nội dung cực đoan, bạo lực và lạm dụng trẻ em – những thứ bị nghiêm cấm và lên án mạnh mẽ.
- **Dịch vụ bất hợp pháp:** Thuê hacker, rửa tiền, thậm chí các tin đồn về dịch vụ ám sát, bắt cóc (mặc dù tính xác thực của nhiều dịch vụ này còn gây tranh cãi và có thể là lừa đảo).
- **Lừa đảo và mã độc:** Do tính chất không được kiểm soát, Dark Web chứa đầy các trang web lừa đảo và là nguồn phát tán mã độc nguy hiểm.

Những lời đồn về các video hành quyết, buôn bán người, hay bán nội tạng trên Dark Web không phải là không có cơ sở, dù rằng việc xác minh mức độ phổ biến và tính xác thực của từng trường hợp cụ thể là rất khó khăn. Điều quan trọng cần nhận mạnh là việc truy cập và tham gia vào các hoạt động bất hợp pháp trên Dark Web không chỉ nguy hiểm mà còn vi phạm pháp luật và có thể dẫn đến những hậu quả nghiêm trọng.

4. Cách sử dụng sao cho hiệu quả và an toàn.

Việc nói về "sử dụng hiệu quả" Deep Web và Dark Web cần được tiếp cận một cách rất thận trọng, đặc biệt là với Dark Web.

a. Sử dụng Deep Web:

- Như đã giải thích, chúng ta sử dụng Deep Web hàng ngày một cách hợp pháp và hiệu quả khi truy cập email, tài khoản ngân hàng, các cơ sở dữ liệu học thuật, thư viện trực tuyến, hay các dịch vụ đám mây.
- **Hiệu quả:** Nằm ở việc khai thác các nguồn tài nguyên thông tin khổng lồ và các dịch vụ trực tuyến được bảo vệ. Các nhà nghiên cứu, sinh viên, chuyên gia sử dụng Deep Web để truy cập các bài báo khoa học, dữ liệu chuyên ngành mà không thể tìm thấy trên Surface Web.

- **An toàn:** Tuân thủ các biện pháp bảo mật cơ bản như sử dụng mật khẩu mạnh, xác thực hai yếu tố, cẩn trọng với các email lừa đảo (phishing), và đảm bảo kết nối an toàn khi truy cập thông tin nhạy cảm.

b. Sử dụng Dark Web:

Việc sử dụng Dark Web tiềm ẩn nhiều rủi ro hơn đáng kể và không được khuyến khích cho người dùng phổ thông. Tuy nhiên, dưới góc độ học thuật và nghiên cứu, có một số khía cạnh được ghi nhận:

- **Tính ẩn danh và tự do ngôn luận:** Dark Web có thể được sử dụng bởi các nhà báo, nhà hoạt động nhân quyền, người tố giác ở những quốc gia có chế độ kiểm duyệt Internet hà khắc để giao tiếp và chia sẻ thông tin một cách ẩn danh, tránh sự theo dõi của chính phủ. Đây là một trong những mục đích ban đầu khi công nghệ Tor được phát triển.
- **Nghiên cứu về an ninh mạng và tội phạm mạng:** Các chuyên gia an ninh mạng và cơ quan thực thi pháp luật có thể (và thực tế là có) theo dõi Dark Web để thu thập thông tin tình báo về các mối đe dọa mạng, các nhóm tội phạm và các hoạt động bất hợp pháp.
- **Bảo vệ quyền riêng tư:** Một số người dùng tìm đến Dark Web vì muốn bảo vệ quyền riêng tư tuyệt đối khi lướt web, tránh bị theo dõi bởi các công ty quảng cáo hoặc các thực thể khác.

Tuy nhiên, để "sử dụng" Dark Web một cách có cân nhắc (và nhấn mạnh là với mục đích hợp pháp và có ý thức cao về rủi ro), cần tuân thủ các nguyên tắc an toàn nghiêm ngặt:

Hiểu rõ rủi ro: Nhận thức đầy đủ về các mối nguy hiểm tiềm ẩn, bao gồm mã độc, lừa đảo, nội dung bất hợp pháp và gây sốc, cũng như sự theo dõi của các cơ quan chức năng đối với các hoạt động phạm pháp.

Sử dụng phần mềm chuyên dụng và cập nhật: Chỉ truy cập Dark Web thông qua các trình duyệt được thiết kế cho mục đích này (như Tor Browser) và luôn đảm bảo chúng được cập nhật phiên bản mới nhất để vá các lỗ hổng bảo mật.

Sử dụng Mạng riêng ảo (VPN): Kết hợp Tor Browser với một dịch vụ VPN uy tín có thể cung cấp thêm một lớp bảo vệ và ẩn danh, mặc dù điều này vẫn còn là chủ đề tranh luận về hiệu quả tuyệt đối trong giới chuyên gia.

Không tải xuống hoặc nhấp vào các liên kết đáng ngờ: Đây là con đường phổ biến để mã độc xâm nhập vào thiết bị.

Tuyệt đối không cung cấp thông tin cá nhân: Giữ danh tính hoàn toàn ẩn danh.

Tránh xa các nội dung và hoạt động bất hợp pháp: Việc xem, tải xuống hoặc tham gia vào các hoạt động này có thể dẫn đến hậu quả pháp lý nghiêm trọng.

Cẩn trọng tối đa: Luôn cảnh giác và không tin tưởng bất cứ điều gì hoặc bất kỳ ai trên Dark Web.

Đối với đại đa số người dùng Internet, việc "sử dụng hiệu quả" Dark Web đồng nghĩa với việc hiểu rõ nó là gì, những nguy cơ của nó và tránh xa nó. Sự tò mò không nên dẫn đến những hành động có thể gây hại cho bản thân hoặc vi phạm pháp luật.

KẾT LUẬN

Deep Web và Dark Web là những phần không thể tách rời của Internet, mỗi phần có những đặc điểm và mục đích riêng. Trong khi Deep Web chủ yếu chứa các nội dung hợp pháp và cần thiết, thì Dark Web, dù có một số ứng dụng hợp pháp trong việc bảo vệ quyền riêng tư và tự do ngôn luận, lại tiềm ẩn vô số nguy cơ và là nơi trú ẩn của nhiều hoạt động tội phạm.

Những lời đồn thổi về sự nguy hiểm của "nơi đen tối nhất trên Internet" phần lớn nhắm vào Dark Web. Việc hiểu đúng, phân biệt rõ ràng và tiếp cận một cách có ý thức, tuân thủ pháp luật và các nguyên tắc an toàn là vô cùng quan trọng. Đối với hầu hết người dùng, việc khai thác các tài nguyên phong phú và hợp pháp của Surface Web và Deep Web là đủ cho nhu cầu hàng ngày, trong khi việc khám phá Dark Web nên được dành cho các chuyên gia có mục đích cụ thể, hợp pháp và được trang bị đầy đủ kiến thức cũng như công cụ bảo vệ.

NGƯỜI BÁO CÁO

Hoàng Xuân Trường