نقد و نظر
فصلنامه علمی‌پژوهشی فلسفه والاهیات
سال بیستم، شماره دوم، تابستان ۱۳۹۴
Naqd va Nazar
The Quarterly Jornal of Philosophy & Theology
Vol. 20, No. 2, Summer, 2015

هک‌کردن و نفوذ به سیستم‌های رایانه‌ای از منظر اخلاقی

علیرضا آل‌بویه *
زینب آل‌بویه **

چکیده

استفاده از سیستم‌های رایانه‌ای و اتصال آنها از طریق شبکه و اینترنت، منجر به ایجاد مشکلات امنیتی بسیاری در رایانه‌ها شده است. توسعه روز افزون فناوری‌ها و روند فزاینده اتکای انسان‌ها به رایانه‌ها برای انجام کارهای حیاتی خود، حاکی از آن است که مشکلات امنیتی آینده ممکن است پیامدهای جدی‌تری را نسبت به رخدادهای امروزی در پی داشته باشد. یکی از تأثیرگذارترین مهارت‌ها برای برقراری امنیت در فضای مجازی، مهارت هک‌کردن و نفوذ به سیستم‌ها است. هک انواع مختلفی دارد که بنظر می‌رسد برخی از آنها اخلاقی و برخی غیراخلاقی باشند. ملاک اخلاقی‌بودن یا نبودن هک می‌تواند انگیزه هکر و چگونگی استفاده او از این مهارت باشد. برخی از افراد می‌گویند تا زمانی که هک هیچ آسیب جدی در پی نداشته باشد، نفوذ می‌تواند موجب توسعه امنیت سیستم‌ها شود، اما بسیاری از افراد با این نظر مخالف بوده و معتقدند که نفوذ تقریباً همیشه آسیب‌رسان بوده و اشتباه است. با توجه به تأثیر امنیت فضای مجازی در زندگی روزمره انسان‌ها و نیز اهمیت زیست اخلاقی، در این مقاله به بررسی هک‌کردن از منظر اخلاقی پرداخته می‌شود.

کلیدواژه‌ها

اخلاق حرفه‌ای، امنیت، اخلاق هک، حریم خصوصی، هکر، فضای مجازی.

* استادیار پژوهشگاه علوم و فرهنگ اسلامی alireza.alebouyeh@gmail.com
** کارشناسی ارشد مهندسی کامپیوتر و پژوهشگر جامعة الزهرا 3 z.alebouyeh@gmail.com

مقدمه

رشد روزافزون فناوری‌ها و اتکای سازمان‌ها و دولت‌ها به آنها سبب ایجاد مسائل امنیتی و اخلاقی جدیدی در حوزه فناوری اطلاعات شده است. مایک مارتین (Mike Martin) می‌گوید: «فناوری تأثیر عمیقی در جهان معاصر دارد و مهندسان نقش محوری در توسعه فناوری دارند. برای حفظ ایمنی، سلامت و رفاه جامعه، مهندسان باید تعهد اخلاقی داشته باشند تا بتوانند با مسائل دشوار اخلاقی که با آنها مواجه می‌شوند، دست و پنجه نرم کنند» (Martin, 2005: xiii).

امروزه عملکرد صحیح سازمان‌ها و دولت‌ها به امنیت و صحت اطلاعاتی وابسته است که در رایانه‌ها ذخیره شده است که در صورت نفوذ به این سیستم‌ها و دسترسی به اطلاعات آنها، آسیب‌های جدی و جبران‌ناپذیری به عملکرد سازمان‌ها و دولت‌ها وارد می‌شود و حتی گاهی ممکن است امنیت ملی به خطر افتد. یکی از چالش‌هایی که فناوری اطلاعات با آن مواجه است، مسئله هک‌کردن رایانه‌ها و شبکه‌ها است.

کارشناسان امنیتی سازمان‌ها با نفوذ به سیستم‌ها و شبکه سازمان می‌توانند نقاط آسیب‌پذیر سیستم‌ها را پیدا کرده و به این ترتیب، راهکارهایی را برای افزایش امنیت شبکه ارائه دهند. بنابراین، مهارت هک و نفوذ مانند یک شمشیر دو لبه است و به همان میزان که می‌تواند برای امنیت سیستم‌ها مفید باشد، نیز می‌تواند تهدید بزرگی برای آنها به‌شمار آید.

در سال‌های اخیر به دلایل مختلفی هک و نفوذ به رایانه‌ها به طور چشم‌گیری افزایش یافته است و می‌توان گفت تقریباً هیچ سیستمی از دست هکرها و نفوذهایشان در امان نیست. برخی افراد که در دنیای واقعی به حریم خصوصی افراد و حقوق آنها احترام می‌گذارند، به محض ورود به فضای مجازی به‌راحتی حریم خصوصی افراد را نقض کرده و به خود اجازه می‌دهند که بدون اجازه وارد سیستم دیگران شده و اطلاعات آنها را بررسی کنند. اغلب هکرها ادعا می‌کنند که کارهای آنها غیراخلاقی نیست، چون به انسان‌ها صدمه نمی‌زند.

گفتنی است امروزه بحث اخلاق هک‌کردن از منظرهای مختلفی از جمله منظر عقلی و الهیاتی بررسی می‌شود که در این مقاله تنها از منظر عقلی به این موضوع پرداخته‌ایم؛ گرچه جنبه‌های مختلف این بحث به لحاظ الهیاتی نیز زمینه‌کار بسیاری دارد.

لزوم بررسی اخلاق هک‌کردن

در سال‌های اخیر به دلایل مختلفی جرایم سایبری و نفوذ به سیستم‌ها به طور چشمگیری افزایش یافته است. هکرها برای انجام‌دادن اعمال خود انگیزه‌های مختلفی دارند. برخی از آنها برای سرقت و انتقام، برخی برای به‌دست آوردن مهارت‌های لازم در برنامه‌نویسی و پیداکردن نقص‌های امنیتی سیستم‌ها و برخی دیگر برای به‌دست آوردن اطلاعات به سیستم‌ها نفوذ می‌کنند. بدون در نظرگرفتن دلایل و انگیزه‌های آنها برای نفوذ به سیستم‌ها، هک‌کردن آسیب‌ها و خسارت‌های زیادی به جامعه وارد می‌کند. این خسارت‌ها شامل از دست‌دادن اطلاعات و فاش‌شدن اطلاعات محرمانه، نقض حریم خصوصی، نادیده‌گرفتن مالکیت معنوی، خسارت‌های اقتصادی و... است.

در مورد از دست‌دادن اطلاعات، هکرها پس از نفوذ به سیستم‌ها، در بسیاری از موارد داده‌ها را تغییر می‌دهند و یا آنها را از روی سیستم حذف می‌کنند. از دست‌دادن اطلاعات و یا فاش شدن اطلاعات محرمانه می‌تواند موجب ایجاد مسائل امنیتی بسیار مهمی گردد. حتی سازمان‌های بزرگی همچون پلیس بین‌الملل، پنتاگون[1] و ناسا[2] هم در طی سال‌های گذشته بارها درگیر این مسائل بوده‌اند.[3]

در مورد حریم خصوصی افراد، زمانی که هکرها به سیستم‌ها نفوذ می‌کنند، می‌توانند به کلیه اطلاعات درون آنها دسترسی داشته باشند. از آنجا که اطلاعات ذخیره‌شده در سیستم‌ها اطلاعات شخصی، حرفه‌ای و حتی اطلاعات مالی افراد است، با از دست‌دادن این اطلاعات خصوصی آسیب‌های زیادی به افراد می‌رسد. نقض حریم خصوصی افزون بر خسارت‌های مالی در بسیاری از موارد صدمات روانی جبران‌ناپذیری را نیز برای افراد به وجود می‌آورد.

---

۱. مرکز و مقر فرماندهی وزارت دفاع ایالات متحده آمریکا (Pentagon)

۲. ناسا (National Aeronautics and Space Administration (NASA)) مخفف سازمان ملی هوانوردی و فضایی آمریکا است که مجری طرح‌های ملی ایالات متحده در زمینه برنامه‌های فضایی و همچنین مسئول مدیریت و اجرای پژوهش‌های تجاری و نظامی در زمینه هوا ـ فضاست.

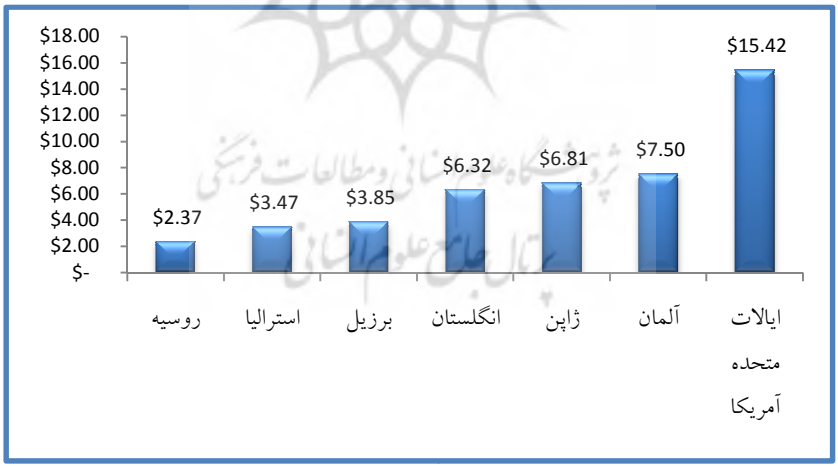
۳. برای مثال، در آگوست ۲۰۱۵م. هکرهای روسی ایمیل‌های پنتاگون را هک کرده و هکرها توانسته‌اند به ایمیل‌های کارمندان نظامی و غیرنظامی شاغل در پنتاگون دسترسی پیدا کنند.
(http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/)

همچنین هکرهای ایرانی (شرکت امنیتی آشیانه) در سال ۱۳۸۵ سایت ناسا را هک کردند
(http://www.ashiyane.ir/archive.php?id=2).

شاید مشخص‌ترین خسارتی که ممکن است با نفوذ به سیستم‌ها رخ دهد، خسارت اقتصادی است. شرکت HP، یکی از معتبرترین شرکت‌ها در زمینه فناوری اطلاعات، در سال ۲۰۱۵م. بر فعالیت‌های ۵۸ سازمان در بخش‌های خصوصی و دولتی آمریکا مطالعاتی انجام داد و در این مطالعات به بررسی خسارت‌های اقتصادی ناشی از جرایم سایبری و هک در کشورهای مختلف پرداخت. این مطالعات که در کشورهای آمریکا، انگلستان، آلمان، استرالیا، ژاپن، روسیه و برزیل صورت گرفت، نشان داد که تعداد و شدت حملات در سال‌های اخیر افزایش یافته است. این حملات شامل سرقت حق مالکیت معنوی سازمان‌ها، مصادره حساب‌های بانکی آنلاین، ایجاد و پخش ویروس‌ها در رایانه‌های دیگر، انتشار اطلاعات تجاری محرمانه در اینترنت و اختلال در زیرساخت‌های ملی و حیاتی یک کشور است (2015 Costs of Cyber Crime Study: United States, 2).

هزینه‌ای که سازمان‌ها در برابر حملات سایبری پرداخت می‌کنند، شامل هزینه‌های تشخیص حملات، مدیریت و اجرای واکنش مناسب در برابر حمله و بازیابی اطلاعات سیستم‌ها می‌شود. خسارت دیگر در اثر حملات به سازمان‌ها و شرکت‌ها، از دست‌دادن مشتریان پس از هر حادثه است که چه‌بسا به دست‌آوردن اعتماد و جلب رضایت آنها کار دشواری باشد (ibid).

این مطالعه بر روی ۲۵۰ سازمان از کشورهای ذکر شده صورت گرفته است. نمودار زیر خسارت‌های اقتصادی ناشی از جرایم سایبری در این کشورها را نشان می‌دهد (ibid.: 3).



نمودار ش ۱: خسارت‌های اقتصادی ناشی از جرایم سایبری در کشورها (ibid.: 4).[۱]

۱. (اعداد بر حسب میلیون دلار است).

نمودار فوق نشان می‌دهد که بیشترین هزینه‌های اقتصادی ناشی از جرایم سایبری در ایالات متحده آمریکا و نزدیک به ۱۵ میلیون دلار و کمترین خسارت برای روسیه بوده است. خسارت‌های ناشی از هک و جرایم سایبری منحصر در شرکت‌های اقتصادی نبوده، بلکه بر تمام سازمان‌های خصوصی و دولتی تأثیر نهاده است و تقریباً هیچ سازمان و شرکتی از نفوذ هکرها در امان نبوده است. نمودار شماره ۲ افزایش خسارت‌های اقتصادی ناشی از جرایم سایبری در سال ۲۰۱۵ نسبت به متوسط خسارت‌ها در ۶ سال گذشته را نشان می‌دهد (ibid.: 11).

نمودار ش۲: هزینه سالانه جرایم رایانه‌ای برای بخش‌های مختلف (ibid.:11).

با توجه به آسیب‌های فردی، اجتماعی، فرهنگی و اقتصادی ناشی از هک و کافی‌نبودن بازدارندگی قوانین جرایم رایانه‌ای و همچنین با در نظر داشتن این نکته که هکرها معمولاً به‌گونه‌ای عمل می‌کنند که قابل شناسایی نباشند و اعمال آنان نیز تا حدودی قابل ردیابی در مراجع قضایی نیست، نیاز به بررسی اخلاقی این موضوع به‌شدت احساس می‌شود، چون ضمانت اجرای اخلاق، وجدان درونی افراد است، برخلاف حقوق که ضمانت اجرای آن بیرونی است. افزون بر اینکه برخی از هکرها حتی کار خود را اخلاقی نیز جلوه می‌دهند. حال برای روشن‌شدن موضوع، به بررسی انواع هکرها می‌پردازیم.

انواع هکرها

هکرها بر اساس نوع فعالیت و اهدافشان به سه دسته اصلی تقسیم می‌شوند:

هکرهای کلاه‌سفید

هکرهای کلاه‌سفید (White hat hackers) هکرهایی هستند که با نیت خوب به سیستم‌ها نفوذ می‌کنند. دلیل کار این هکرها بررسی امنیت سیستم‌هاست که در جامعه امنیت رایانه‌ای به آن تست نفوذ (Penetration Test) می‌گویند. به این هکرها هکرهای قانون‌مند یا هکرهای اخلاقی (Ethical Hacker) نیز می‌گویند و حتی در سراسر دنیا مدارک معتبری نیز با عنوان «گواهی‌نامه هک قانون‌مند» (Certified Ethical Hacking (CEH)) وجود دارد. این افراد غالباً به‌عنوان کارشناسان امنیتی در سازمان‌ها و شرکت‌ها مشغول به کار می‌شوند (Graves, 2010: 4). این افراد با شرکت‌ها و سازمان‌ها قرارداد بسته و تلاش می‌کنند تا با رعایت کلیه اصول هک اخلاقی به سیستم‌ها نفوذ کرده و نقاط ضعف آنها را شناسایی کنند. این گروه به هکرهای خوب معروف‌اند و نه‌تنها برای جامعه مضر نیستند، بلکه به امن‌کردن سیستم‌ها کمک می‌کنند. معمولاً هکرهای کلاه‌سفید در سراسر دنیا به صورت آزادانه و قانونی به فعالیت می‌پردازند (Young, 2004: 66).

هکرهای کلاه‌سفید در واقع بر دو گروه‌اند: گروه اول کارشناسان امنیتی سازمان‌ها هستند و جزو کارمندان سازمان‌ها به‌شمار می‌آیند. این گروه برای اینکه امنیت سیستم‌ها و شبکه سازمان را بررسی کنند و نقاط ضعف امنیتی آنها را به دست آورند، باید در کلیه سیستم‌های سازمان تست نفوذ انجام دهند. تست نفوذ در واقع یافتن نقاط ضعف سیستم‌ها و راه‌های نفوذ به آنهاست. البته در این نفوذها هیچ‌گونه آسیبی به سیستم‌ها نمی‌رسد. این گروه از هکرها برای انجام‌دادن تست نفوذ از مقام عالی‌رتبه سازمان اجازه کتبی دریافت می‌کنند و به‌هنگام اتمام کار تست نفوذ در سیستم‌ها، با ارائه گزارشی نقاط ضعف سیستم‌ها و شبکه سازمان را به اطلاع مدیر سازمان و مسئول فناوری اطلاعات سازمان می‌رسانند تا برای امن‌کردن سیستم‌ها و زدودن نقاط ضعف امنیتی آنها اقدام گردد.

گروه دوم هکرهای کلاه‌سفید افرادی هستند که جزو کارمندان سازمان‌ها نیستند، بلکه عضو شرکت‌های امنیتی هستند که برای انجام‌دادن تست نفوذ روی سیستم‌های سازمان‌ها با

آنها قرارداد می‌بندند و پس از دریافت مجوز کتبی از مقام عالی سازمان کار خود را شروع می‌کنند. شیوه کار این گروه نیز دقیقاً شبیه گروه اول است. با توجه به مطالب پیش‌گفته مشخص است که اعمال هکرهای کلاه‌سفید به دلیل اینکه با اجازه مدیر سازمان‌ها و طبق قانون صورت می‌گیرد و هیچ آسیبی هم به سیستم‌ها نمی‌رساند، از لحاظ اخلاقی درست است.

هکرهای کلاه‌سیاه

هکرهای کلاه‌سیاه (Black hat hackers) افرادی هستند که با نیت‌های غیراخلاقی به سیستم‌ها نفوذ کرده و کارهای مخرب انجام می‌دهند. این گروه از هکرها طبق قوانین مجرم شناخته می‌شوند. این گروه، خراب‌کارترین نوع هکرها هستند که پس از نفوذ به رایانه‌ها اطلاعات آنها را سرقت کرده و یا تخریب می‌کنند (Young, 2004: 67; Graves, 2010: 4).

نیّت هکرهای کلاه‌سیاه، سرقت، خراب‌کاری و ایجاد اختلال، انتقام، جعل اطلاعات، شنود و دستکاری اطلاعات است. اغلب اعمال هکرهای کلاه‌سیاه سبب خسارت‌های مالی و حتی جانی می‌شود. این هکرها گاهی برای جاسوسی دولت‌ها و شرکت‌ها نیز استخدام می‌شوند. بنابراین، نفوذ هکرهای کلاه‌سیاه به لحاظ اخلاقی نادرست است؛ هم به این دلیل که نیت سوء داشته‌اند و هم اینکه خود اعمالشان نیز به لحاظ اخلاقی نادرست بوده است، چون سرقت، خراب‌کاری، انتقام، جعل اطلاعات و.... به خودی خود به لحاظ اخلاقی نادرست است. به بیان دیگر، نه‌تنها در هکرهای کلاه‌سیاه حسن فاعلی در کار نیست، بلکه حسن فعلی نیز تحقق ندارد.

هکرهای کلاه‌خاکستری

هکرهای کلاه‌خاکستری (Gray hat hackers) در میان هکرهای کلاه‌سفید و کلاه‌سیاه هستند. این گروه از هکرها از داده‌های دیگر سیستم‌ها بهره می‌برند، ولی صدمه‌ای به سیستم وارد نمی‌کنند. آنها غالباً به نیت یادگرفتن چیزهای جدید و کنجکاوی‌های فنی در اینترنت جست‌وجو کرده و وضعیت امنیتی سایت‌ها و سرورها را بررسی می‌کنند (Young, 2004: 66). هکرهای کلاه‌خاکستری گاهی با کشف یک نقص امنیتی آن را به مدیر آن سیستم اطلاع می‌دهند و حتی گاهی پیشنهاد همکاری برای حل مشکل را نیز به مدیر سیستم می‌دهند.

یکی از تفاوت‌های اصلی میان هکرهای کلاه‌خاکستری با هکرهای کلاه‌سفید، موضوع «اجازه» خواستن است. چه‌بسا نیت یک هکر کلاه‌خاکستری خوب باشد، ولی نکته مهم این است که او بدون اجازه وارد سیستم و حریم خصوصی دیگران می‌شود (Graves, 2010: 4).

بسیاری از هکرهای کلاه‌خاکستری تصدیق می‌کنند که چه‌بسا کپی‌کردن، دست‌کاری‌کردن و تغییردادن اطلاعات رایانه‌ها نادرست باشد و در مواقعی حتی به افراد آسیب برساند، ولی می‌گویند از طریق نفوذ به سیستم‌ها، به رایانه‌ها و اطلاعات درون آنها هیچ آسیبی نمی‌رسانند. از نظر هکرهای کلاه‌خاکستری عمل هک‌کردن از نظر اخلاقی نادرست نیست، ولی ممکن است استفاده از اطلاعات به‌دست‌آمده از طریق هک‌کردن نادرست باشد.

استدلال‌های هکرهای کلاه‌خاکستری

هکرهای کلاه‌خاکستری برای توجیه اخلاقی نفوذهای خود، استدلال‌هایی را بیان می‌کنند که در ادامه به بررسی و نقد آنها پرداخته می‌شود.

استدلال اول: آزادی اطلاعات

یکی از مشهورترین استدلال‌های هکرها برای توجیه مجاز بودن نفوذهای خود، آزادی اطلاعات است. اغلب هکرها از اصول اخلاقی‌ای پیروی می‌کنند که هم رفتار آنها را هدایت کرده و هم نفوذهایشان را به لحاظ اخلاقی توجیه می‌کند. طبق این اصول اخلاقی، همه اطلاعات باید آزاد باشد. اصول اخلاقی هکرها که لوی (Levy) در سال ۱۹۸۴ ارائه داده است عبارتند از:

الف) دسترسی به رایانه‌ها و هر چیزی که ممکن است به افراد چیزی را در مورد چگونگی کارکرد جهان بیاموزد، باید نامحدود و کامل باشد.

ب) تمام اطلاعات باید برای عموم افراد آزاد و در دسترس باشد و از پنهان‌کاری باید اجتناب شود (Levy, 1994: 33).

به گفته کلاه‌خاکستری، انگیزه اولیه آنها برای نفوذ به سیستم‌ها یادگیری بیشتر در مورد چگونگی کارکرد سیستم‌ها، اشکال‌زدایی و توسعه امنیت آنهاست، نه آسیب‌زدن به سیستم‌ها. آنها برای یادگیری نیاز دارند که به اطلاعات و منابع شبکه دسترسی داشته باشند. در واقع هکرها به یادگیری و کنجکاوی در رایانه‌ها علاقه شدیدی دارند. حال اگر شما به

اطلاعاتی که برای یادگیری و توسعه امنیت سیستم‌ها لازم است دسترسی نداشته باشید، چگونه می‌توانید سیستمی را تعمیر کنید یا امنیت آن را توسعه دهید؟ بنابراین، از دیدگاه هکرها باید سیستمی باز داشته باشیم که دسترسی به اطلاعات برای همه آزاد باشد و هیچ مرزی میان یک هکر و اطلاعات و تجهیزات مورد نیاز که او برای افزایش دانش خود و توسعه سیستم‌ها وجود نداشته باشد (Denning, 1990: 4,5).

ادعای اصلی نظریه‌پردازان آزادی اطلاعات این است که ما برای تصمیم‌گیری در تمامی جنبه‌های زندگی خود به اطلاعات نیاز داریم. در تصمیم‌گیری برای خرید یک ماشین مناسب، در تصمیم‌گیری برای انتخاب رشته دانشگاهی و یا برای انتخاب شایسته میان کاندیداهای انتخابات، ما به اطلاعاتی مانند اطلاعات فنی اتومبیل‌ها، چشم‌انداز شغلی در رشته‌های مختلف و یا رزومه کامل در مورد هر کدام از کاندیداهای انتخاباتی نیاز داریم (Jennings, 1992: 8). در غیر این صورت، نمی‌توانیم انتخابی منطقی و به‌هنگام داشته باشیم. استدلال آزادی اطلاعات چهار اشکال عمده دارد:

این استدلال در مورد تمام اطلاعات صدق نمی‌کند. درست است که برای تصمیم‌گیری‌های درست، باید برخی از اطلاعات آزاد باشند، ولی ارزش‌های انسانی و ارزش‌های جامعه ما با آزادی کامل اطلاعات ناسازگار است. سه دسته اطلاعات نباید آزادانه در دسترس باشند:

الف) حریم خصوصی افراد: حریم خصوصی حقی است که همه افراد برای آن احترام قائل‌اند. اطلاعات حساب‌ها و کارت‌های بانکی، اطلاعات و عکس‌های خانوادگی، نتیجه پژوهش‌های افراد و... از اطلاعاتی هستند که جزو حریم خصوصی افرادند و نباید به‌سادگی در اختیار دیگران قرار گیرند، چون در غیر این‌صورت، امنیت مالی و روانی افراد تحت تأثیر قرار خواهد گرفت.

ب) امنیت ملی: برخی اطلاعات طبقه‌بندی شده دفاعی و ملی کشورها باید محرمانه بمانند، در غیر این‌صورت، امنیت ملی آنها به خطر می‌افتد.

ج) سرمایه‌داری و ارزش اطلاعات: اگر امکان مخفی نگه‌داشتن اطلاعات تجاری وجود نداشته باشد، فضای رقابتی و توسعه از میان خواهد رفت و بی‌گمان سیستم اقتصادی با مشکل مواجه خواهد شد (Jennings, 1992: 8,9).

اعتقاد به این دیدگاه، نقض حریم خصوصی را در پی خواهد داشت. این دیدگاه موجب پیدایش مسائل نگران‌کننده‌ای درباره حریم خصوصی می‌شود؛ یعنی اگر تمام اطلاعات آزاد باشد، دیگر حریم خصوصی‌ای وجود ندارد و هر کسی که بخواهد می‌تواند به خصوصی‌ترین اطلاعات افراد دسترسی داشته باشد (Spafford, 1992: 4).

اشکال دیگر این استدلال، خدشه وارد کردن به درستی اطلاعات است. امروزه اعتماد انسان‌ها و سازمان‌ها به فناوری اطلاعات و رایانه‌ها روز به روز بیشتر می‌شود و کلیه اطلاعات، حتی حیاتی‌ترین و سرّی‌ترین آنها در رایانه‌ها ذخیره می‌شوند. این اطلاعات شامل اطلاعات بانک‌ها، سازمان‌های پزشکی، سازمان‌های دولتی، اطلاعات نظامی، دفاعی و... است. بنابراین، جامعه ما بر اطلاعاتی مبتنی است که درستی آنها باید تضمین‌شده باشد و حال آنکه آزادی اطلاعات به این معناست که هر کسی می‌تواند به اطلاعات دسترسی داشته و در صورت لزوم حتی آنها را تغییر دهد. پس دیگر مالکیتی برای اطلاعات وجود نخواهد داشت و پدیدآورندگان اطلاعات هیچ حقی برای نگهداری و بهره‌برداری از آنها ندارند.

اطلاعات بانکی، اطلاعات پزشکی، اطلاعات دفاعی و... از مواردی هستند که همواره باید درستی آنها مراقبت شود. پس اگر لازم باشد کسی درستی اطلاعات و دسترسی افراد به چنین اطلاعاتی را مراقبت کند، مشخص است که اطلاعات دیگر آزاد نیست. اگر چنین کنترلی وجود نداشته باشد، به‌طبع نمی‌توانیم به درستی اطلاعات اعتماد کنیم. به‌سادگی قابل تصور است که چنین فلسفه‌ای چه قدر آسیب و هرج و مرج در دنیای ما ایجاد خواهد کرد. بی‌گمان در دنیایی که امکان وجود افراد بی‌دقت و غیراخلاقی وجود دارد، «آزاد»دانستن تمام اطلاعات غیر اخلاقی است (Spafford, 1992: 4).

چهارمین اشکال استدلال آزادی اطلاعات، نقض مالکیت معنوی است. مطابق این استدلال، دیگر مفهوم مالکیت معنوی وجود نخواهد داشت. فردی که با صرف هزینه و زمان زیاد اطلاعاتی را جمع‌آوری کرده و یا نرم‌افزاری را نوشته است، این اطلاعات و یا نرم‌افزار به‌طبع دارایی او به‌شمار می‌آید، ولی ادعای آزادی اطلاعات، دیگر مالکیتی برای فرد قائل نیست و این امر به نابودی ارزش‌های اخلاقی، زیان اقتصادی و جلوگیری از بروز خلاقیت در جامعه خواهد انجامید (Spafford, 1992: 4؛ Tavani, 2004:159؛ سعیدی، ۱۳۹۲: ۱).

بنابراین، مطابق استدلال‌های اقتصادی نیز می‌توان چنین فلسفه‌ای را به چالش کشید. در نتیجه استفاده از این دیدگاه خام برای توجیه نفوذهای رایانه‌ای و اخلاقی نشان دادن آنها آشکارا نادرست است.

استدلال دوم: استدلال امنیتی

این استدلال رایج‌ترین استدلالی است که هکرهای کلاه‌خاکستری برای توجیه اخلاقی نفوذهای خود به کار می‌برند. به باور بسیاری ازآنها که فعالیت‌هایشان نه‌تنها به زیان جامعه نیست، بلکه با آشکارکردن نقاط ضعف سیستم‌ها به سود امنیت سیستم‌ها و جامعه است (Baird, 1987: 7). در واقع، دفاع رایج آنان این است که آنها تنها برای تست امنیتی و شناسایی نقاط ضعف امنیتی سیستم‌ها به آنها نفوذ می‌کنند. مطابق این استدلال، برخی از هکرها امن‌کردن سیستم‌های دیگران را وظیفه خود می‌دانند و برای انجام‌دادن این کار بدون اجازه آنها به سیستم‌هایشان نفوذ می‌کنند. این افراد اعتقاد دارند که با انجام این کار، به ارائه یک خدمت عمومی می‌پردازند و از همین‌رو، اعمال آنها به لحاظ اخلاقی درست باشد.

اشکالات استدلال امنیتی

بر این استدلال نیز اشکال‌هایی وارد کرده‌اند؛ از جمله اینکه:

۱. این ادعا که «من تنها امنیت سیستم را بررسی می‌کنم و به آن آسیب نمی‌رسانم» دفاعی معتبر نیست. تصورکنید به خانه برگشته‌اید و این یادداشت را روی در یخچال خود مشاهده می‌کنید: «من امنیت کلیه درهای خانه شما را بررسی کردم و متوجه شدم که قفل یکی از درهای شما خراب است. نگران نباشید من هیچ چیزی برنداشتم. شما برای امنیت خانه خود باید قفل درب خود را تعمیر کنید». آیا با دیدن این مطلب شما احساس نمی‌کنید که به خانه شما تجاوز کرده‌اند؟ بی‌گمان شما چنین احساسی را خواهید داشت (Fötinger, 2004: 4,5). درست است که چیزی از وسایل خانه شما به سرقت نرفته و به‌ظاهر نیت فرد واردشده به خانه خیر بوده است، ولی شما پس از دیدن آن یادداشت دیگر در خانهٔ خود احساس امنیت و آرامش نخواهید کرد، چون فردی غیرمجاز به حریم خصوصی خانه شما وارد شده است و حریم خصوصی شما را نقض کرده است.

۲. افرادی که می‌خواهند مشکل امنیتی یک سیستم را گزارش دهند، لازم نیست از

طریق هک‌کردن و آسیب‌رساندن به سیستم‌ها آن مشکل را گزارش کنند. این روش هشدار، دقیقاً مانند آن است که فردی برای هشداردادن امکان خطر آتش‌سوزی در یک مرکز خرید آن مرکز را به آتش بکشد و عمل خود را این‌گونه توجیه کند که اگر چنان نمی‌کردم، آتش‌نشانی به هشدارهای من درباره خطر آتش‌سوزی توجهی نمی‌کرد (Spafford, 1992: 5).

۳. یکی از نقص‌های این استدلال آن است که به طور کامل عوامل فنی و اقتصادی‌ای را که مانع به روزرسانی بسیاری از سایت‌ها و یا اصلاح امنیتی نرم‌افزارشان می‌شود، نادیده می‌گیرد. ممکن است همه سایت‌ها و سازمان‌ها منابع لازم را برای ارتقای امنیتی و رفع نواقص سخت‌افزارها و نرم‌افزارهای خود نداشته باشند. نفوذ به سیستم‌ها با این استدلال که قربانی قفل ضعیفی به کار برده و در نتیجه، گویی خود خواهان آن بوده است که دیگران با نفوذ به سیستم او نقص امنیتی آن را گوشزد کنند، به لحاظ اخلاقی و قانونی موجه نیست (Spafford, 1992: 6). برای مثال، چه‌بسا کارشناس امنیت فناوری اطلاعات در یک سازمان، نقص امنیتی سیستمی را پیدا کرده و مدیران سازمان نیز از این نقص اطلاع دارند، ولی به سب کمبود بودجه در حال حاضر نمی‌توانند نقص امنیتی را برطرف کرده و یا سیستم امنیتی خود را به روز رسانی کنند. در نتیجه، تلاش هکرها در نفوذ به این سیستم‌ها برای وادار کردن صاحبان آنها به ارتقای ساختار امنیتی سیستم‌هایشان، زشت و قابل سرزنش است.

۴. در مورد نفوذ به سیستم‌ها، در نگاه اول شاید تصور شود که نفوذ هکرهایی که قصد هشدار نقص‌های امنیتی سیستم‌ها را دارند، از نظر اخلاقی درست باشد، چون آنها با هشدار به صاحبان سیستم‌ها کمک می‌کنند تا آنها امنیت سیستم خود را ارتقا دهند و از نفوذها و سرقت‌های جدی‌تر و خطرناک‌تر در امان بمانند، اما نکته این است که آیا تمامی پی‌آمدهای قطعی ناشی از یک نفوذ مشخص است؟ آیا این نوع هک‌کردن بیشتر به سود جامعه است یا به زیان آن؟ روشن است که همه پیامدهای ناشی از این نفوذها مشخص نیست (Falk, 2004: 4). برای مثال، چه‌بسا در لحظه‌ای که هکری به سیستمی نفوذ کرده و کار آن را مختل کرده است، آن سیستم از انجام یک فعالیت حیاتی و مهم باز ماند و آسیب‌های مالی و حتی جانی شدیدی به جامعه وارد شود.

اغلب سازمان‌ها و مؤسسه‌ها فردی را به عنوان مسئول امنیت فناوری اطلاعات در نظر

می‌گیرند که وظیفه او تأمین امنیت شبکه و سایت سازمان است. حال فرض کنید هکری به قصد هشدار دادن به مسئولان یک بانک درباره امن‌نبودن سایت اینترنتی بانک‌شان، به سایت آن بانک نفوذ کند. از آنجا که هک‌شدن سایت یک بانک بازتاب گسترده‌ای خواهد داشت و اختلال زیادی در کارها ایجاد می‌کند، ممکن است مسئولان بانک مسئول امنیت فناوری اطلاعات سازمان را توبیخ کنند و حتی در شرایطی به سبب این نفوذ صورت‌گرفته وی را از کار برکنار کنند. بیکار شدن مسئول امنیت فناوری بانک و فشارهای جسمی و روانی‌ای که در پی نفوذ هکر برای وی ایجاد می‌گردد، از پی‌آمدهایی است که یک هکر بدان فکر نکرده است.

یا اینکه چه‌بسا هکری برای هشدار نقص امنیتی سیستم یک بانک، با هک‌کردن سایت بانکی آن را از دسترسی افراد خارج کند و در نتیجه کسی نتواند وارد سایت بانک شده و کارهای بانکی خود را انجام دهد. حال شرایطی را در نظر بگیرید که فردی در مدت زمانی که سایت بانک هک شده است، نیاز دارد که برای اجرای فعالیت تجاری مهمی از طریق سایت حواله اینترنتی ارسال کند و در صورت ارسال‌نکردن حواله، زیان اقتصادی بزرگی به وی وارد می‌شود. این در حالی است که هکر سایت بانکی هرگز به این‌گونه پی‌آمدهای ناشی از نفوذ خود نمی‌اندیشد.

استدلال سوم: استدلال سیستم‌های بلااستفاده

یکی دیگر از استدلال‌های هکرهای کلاه‌خاکستری در توجیه مجازبودن نفوذهایشان، استفاده از منابع بلااستفاده سیستم‌هاست. هکرها اغلب ادعا می‌کنند که آنها به سیستم‌ها هیچ آسیبی نمی‌رسانند، بلکه تنها با بهره‌گیری از منابع بلااستفاده آنها، از هدر رفتن منابع جلوگیری می‌کنند. به گفته آنها توان پردازشی سیستم‌ها بالاست و اغلب کاربران و سازمان‌ها نه‌تنها از تمام توان پردازشی سیستم‌هایشان استفاده نمی‌کنند، بلکه تنها بخش اندکی از توان پردازشی سیستم خود را به کار می‌گیرند (Ethical Hacking: Student Guid, 2000: 27.).

از نظر هکرها، اصلی اخلاقی وجود دارد که هدر رفتن منابع باارزش را در جامعه‌ای که افراد زیادی به آن منابع نیاز دارند محکوم می‌کند. هکرها با استفاده از این اصل کار خود را از نظر اخلاقی توجیه کرده و درست می‌دانند. بیان این مطلب ضروری است که برخی اصول اخلاقی حقوقی از افراد را محدود می‌کند. برای مثال، اصلی اخلاقی وجود دارد که

اجازه می‌دهد افراد در صورت لزوم برای دفاع از خود فردی را بکشند. در این حالت، یک اصل اخلاقی حق حیات را محدود کرده است. طبق استدلال هکرها نیز ممکن است نفوذ و استفاده از سیستم‌های دیگران حق مالکیت آنان را نقض کند، ولی مطابق اصل اخلاقی «جلوگیری از هدر رفتن منابع» محدود می‌شود (Himma, 2008: 229,230). بنابراین، هکرهای کلاه‌خاکستری برای جلوگیری از هدر رفتن منابع، حریم خصوصی و حق مالکیت دیگران را نقض می‌کنند و کار خود را نیز اخلاقی می‌دانند.

اشکالات استدلال سیستم‌های بلااستفاده

بر این استدلال نیز اشکال‌های متعددی وارد است: از جمله اینکه مراد از منابع بلااستفاده چیست؟ سه معنا برای آن متصور است: ۱. در واقع منابع بلااستفاده چندان هم بلااستفاده نیستند، بلکه برای شرایط خاص و بحرانی در نظر گرفته شده‌اند و در شرایط و زمان‌های خاصی بی‌گمان از آنها استفاده خواهد شد؛ مانند در نظر گرفتن توان پردازشی بالا برای سرورهای بانک‌ها؛ ۲. منابع به‌ظاهر بلااستفاده به عنوان منابع یدکی هستند؛ مانند واحد پردازش مرکزی (cpu) یا درایو دیسک سخت (Hard Disk) اضافه در یک سازمان. تفاوت این معنا با معنای قبلی در این است که بر اساس معنای دوم از منابع یدکی تنها در صورت خرابی منابع اصلی استفاده قرار می‌شود، ولی در حالت اول در صورت افزایش درخواست‌ها افزون بر استفاده از ظرفیت اولیه، از کل ظرفیت پردازش سیستم استفاده خواهد شد. از این‌رو، هرگز بر ظرفیت اولیه عنوان یدکی صادق نیست؛ ۳. منابع بلااستفاده در واقع نیز بدون استفاده‌اند و مالکان اصلاً هیچ نیازی به آنها ندارند. در ادامه این سه معنا از منابع بلااستفاده را بررسی می‌کنیم:

اشکال براساس معنای اول منابع بلااستفاده: بسیاری از سیستم‌هایی که بخش زیادی از منابع آنها بلااستفاده است، معمولاً برای فراهم‌کردن محیط کاربری همه‌منظوره نیستند، بلکه برای کاربردهای تجارتی، پزشکی، نظامی، امنیتی، پژوهشی، عملیات دولت و.... استفاده می‌شوند. ظرفیت بلااستفاده این سیستم‌ها اغلب برای نیازهای آینده و موج فعالیت‌هایی در نظر گرفته شده‌اند که ممکن است به‌ناگهان رخ دهند، نه برای پشتیبانی از افراد بیرونی که به این منابع نیاز دارند (Spafford, 1992: 7).

تصور کنید اگر تعداد زیادی از افرادی که به رایانه شخصی با منابع پردازشی مناسب دسترسی ندارند بخواهند از مزایای یک سیستم با ظرفیت پردازشی بی‌کار استفاده کنند. در این حالت، سیستم به‌زودی بار پردازشی اضافه خواهد یافت و کارایی آن به‌شدت چنان تنزل پیدا می‌کند که دیگر حتی نمی‌تواند به مالکان ذی‌حق خود خدمات لازم را ارائه دهد و در نهایت در اثر بار اضافه از دسترس خارج خواهد شد. حال اگر در وضعیت پیش‌آمده صاحبان سیستم به‌ناگهان به استفاده از ظرفیت اضافی سیستم خود نیاز داشته باشند، کوتاه‌کردن دست این افراد و بیرون‌کردن آنها از سیستم دشوار و زمان‌بر خواهد بود. در نتیجه افرادی که هزینه زیادی برای فراهم‌کردن منابع پردازشی سازمان خود پرداخت کرده‌اند، متأسفانه در زمانی که به این توان پردازشی نیاز دارند، نمی‌توانند از آن بهره ببرند.

اشکال بر اساس معنای دوم منابع بلااستفاده: در طراحی سیستم‌های رایانه‌ای بحثی با عنوان طراحی سیستم‌های مطمئن وجود دارد؛ به این معنا که به موازات سخت‌افزارها و نرم‌افزارهای سیستم، سخت‌افزارها و نرم‌افزارها یدکی وجود دارند که در صورت خراب‌شدن منابع اصلی سیستم، منابع یدک فعال خواهند شد. هدف از طراحی سیستم‌های مطمئن، داشتن سیستمی است که هیچ‌گاه از کار نیفتد. از این طراحی بیشتر در سیستم‌های کنترلی و حیاتی استفاده می‌شود. برای مثال، در هواپیما دو موتور وجود دارد که تنها یکی در حال کار کردن است و موتور دیگر موتور یدک است و در مواقعی که برای موتور اول مشکلی پدید بیاید و از کار بیفتد، موتور دوم فعال می‌شود. در طراحی سیستم‌های رایانه‌ای نیز در بسیاری از مواقع از هارد دیسک‌ها، پردازنده‌ها و سیستم‌های یدک استفاده می‌شود که در صورت خرابی هارد دیسک، پردازنده و یا سیستم اصلی، نمونه یدک آنها فعال خواهند شد.

در واقع این منابع بلااستفاده برای داشتن سیستمی مطمئن در نظر گرفته شده‌اند تا در مواقع خرابی قطعات اصلی، فعال شوند و در کارکرد سیستم اختلالی ایجاد نشود. استفاده از این منابع یدک با این استدلال که در حال هدر رفتن هستند، به یقین نادرست است، چون زمانی که برای منابع اصلی مشکلی پدید آید، اگر منابع یدک در حال استفاده باشند سیستم از کار خواهد افتاد. برای مثال، اکثر راننده‌ها همیشه در خودرو خود یک لاستیک یدک

نگهداری می‌کنند تا اگر زمانی برای یکی از لاستیک‌ها مشکلی پدید آمد، لاستیک پنچرشده را با لاستیک یدک تعویض کنند. حال اگر کسی با هدف جلوگیری از هدر رفتن منابع بلااستفاده، لاستیک یدک خودرو را بردارد و راننده آن غافل از این موضوع به مسافرت برود و از قضا در میانه راه یکی از چرخ‌ها پنجر شود. در این وضعیت با وجود اینکه راننده برای چنین مواقعی آینده‌نگری کرده بود و لاستیک یدک تهیه کرده بود، ولی به دلیل اینکه شخص دیگری از لاستیک یدک او استفاده می‌کند، نمی‌تواند به مسیر خود ادامه دهد و در جاده می‌ماند.

اشکال براساس معنای سوم منابع بلااستفاده: اگر این ظرفیت پردازشی بلااستفاده برای استفاده آینده در نظر گرفته نشده باشد و به‌واقع برای صاحب سیستم بلااستفاده باشد، باز هم چنین استدلالی نادرست است. هرچند هکر کلاه‌خاکستری کوشیده است که کار خود را بر اساس اصل اخلاقی «جلوگیری از هدر رفتن منابع» که به گمان او بر اصل اخلاقی حریم خصوصی و حق مالکیت حاکم است، توجیه کند، ولی حتی با این اوصاف نیز استدلال او قابل دفاع نیست. اگر فردی نسبت به شیئی حق مالکیت داشته باشد، دیگران حق ندارند بدون اجازه او و تنها با این استدلال که آن شیء در حال هدر رفتن است، از آن بهره‌مند شوند.

به‌طبع غیرمنطقی است که افرادی هزینه و زمان زیادی را صرف خریداری و نگهداری شیئی کنند و دیگران مدعی شوند زمانی که آن شیء بلااستفاده است، آنها حق استفاده از آن را دارند. برای مثال، تصور اینکه شخصی سوار خودرو گران‌قیمت من شود و تنها به این دلیل که در حال حاضر از خودرو استفاده نمی‌کنم، به‌راحتی با آن رانندگی کند، خنده‌دار است. به همین ترتیب، زمانی که فردی در محل کار خود است، برگزاری مهمانی در منزل او با این استدلال که خانه او در حال حاضر بلااستفاده است، صحیح نیست (Ibid.).

اگر استفاده از خودرو و منزل افراد بدون اجازه آنها و به منظور جلوگیری از اتلاف منابع غیر منطقی است، پس به‌طبع موقعیت‌های مرتبطی که بیان می‌کنند ظرفیت محاسباتی استفاده نشده منابع اشتراکی هستند، و یا نرم‌افزار توسعه‌یافته شخصی من به هر کسی تعلق دارد، موقعیت‌هایی به همان اندازه نادرست (و غیراخلاقی) هستند. هیچ اصل کلی اخلاقی که نقض حق مالکیت را برای جلوگیری از اتلاف توجیه کند، وجود ندارد. پس استدلال

نفوذ به سیستم‌ها به منظور استفاده از منابع بلااستفاده نادرست و غیر اخلاقی است.

به بیان دیگر، اگر بنا باشد در دنیای واقعی نیز چنین اصلی حاکم باشد و انسان مجاز باشد از هر شیء بلااستفاده‌ای استفاده کند، هرج و مرج شدیدی در زندگی اجتماعی پدید می‌آید و هر کسی به خودش حق می‌دهد که اموال بدون استفاده دیگران را به‌کار گیرد. بی‌گمان افراد ثروتمند تنها از بخش کوچکی از ثروتشان به طور شخصی استفاده می‌کنند و این امر موجب نمی‌شود که دیگران به خود حق دهند از اموال بلااستفاده آنها بهره ببرند. بنا بر چنین اصول و اندیشه‌هایی، آیا دیگر جایی برای امور اخلاقی و اصولی مانند حریم خصوصی، حق مالکیت مادی، معنوی و... باقی می‌ماند.

چگونه است که افراد در دنیای حقیقی به خود چنین حقی را نمی‌دهند، ولی در دنیای مجازی به‌راحتی خود را مجاز دانسته و با ارتکاب چنین اعمالی در واقع اصول اخلاقی را به‌آسانی زیر پا می‌گذارند. آیا به‌واقع میان فضای واقعی و فضای مجازی تفاوتی هست؟ آیا جز این است که فضای مجازی نیز به یک معنا در زندگی واقعی ما انسان‌ها رخ می‌دهد و در مرتبه‌ای از واقعیت قرار دارد و در نتیجه، در مراعات‌کردن اصول اخلاقی تفاوتی میان فضای واقعی و فضای مجازی نیست و تنها قوه خیال ما انسان‌هاست که موجب می‌شود در این دو فضا به دو گونه متفاوت عمل کنیم. به بیان دیگر، آیا فضای واقعی اخلاق واقعی، و فضای مجازی اخلاقی مجازی می‌طلبد؟![1]

استدلال چهارم: استدلال محافظان اجتماعی (برادر بزرگ)

جورج اورول (George Orwell) نویسنده معروف انگلیسی، رمانی در سال ۱۹۴۹ نوشت که از پدیدآمدن یک جامعه وحشت‌برانگیز حکایت می‌کرد؛ جامعه‌ای که در آن برادر بزرگ (نماد سیستم حاکم) بر ساحت خصوصی و عمومی افراد جامعه نظارت تام داشت و مهم‌ترین ابزار این نظارت، تلویزیون‌هایی بودند که در همه جا (منزل، اداره‌ها گذرگاه‌ها و...) نصب شده‌اند و کسی قادر و جایز به خاموش‌کردن آنها نیست. در این رمان که عنوان

۱. البته این مسئله که چرا ما انسان‌ها غالباً در دو فضای واقعی و مجازی به دو گونه رفتار می‌کنیم و علل و عوامل وجودشناختی، معرفت‌شناختی و روان‌شناختی آن چیست، موضوع مهمی است که در این مقاله مجال پرداختن به آن نیست.

آن ۱۹۸۴ بود، برادر بزرگ نمادِ نظام حکومتی است که به اشکال گوناگون، بر زندگی طبقات مختلف مردم نظارت و کنترل دارد. این رمان پس از اتمام جنگ جهانی دوم نوشته شد و انگیزه نویسنده در واقع اخطار دادن به غرب در مورد گسترش کمونیسم بود. نویسنده رمان وضعیتی از آینده جامعه را پیش‌بینی می‌کرد که در آن قوانین حکومتی آزادی‌های فردی و حریم خصوصی افراد را به‌شدت پایمال می‌کنند؛ به‌گونه‌ای که حتی مانیتورها در خانه‌ها از شهروندان جاسوسی می‌کنند.[1] البته داستان این رمان را تا حدود زیادی می‌توان به شرایط حاکم بر جوامعی که زیر سلطه حکومت‌های استبدادی‌اند تعمیم داد.

هکرها اعتقاد دارند که پیش‌بینی اورول در جامعه امروز به‌واسطه فناوری و فضای سایبر به واقعیت پیوسته است و این امکان را ایجاد کرده است که برادری بزرگ همه افکار و اعمال ما را زیر نظر داشته باشد. به اعتقاد آنها، افزایش روزافزون قدرت رایانه‌ها برخی نظارت‌ها و کنترل‌های پنهانی را برای جامعه به همراه داشته است. امروزه دستگاه‌های هوشمند در تمام خانه‌ها و مکان‌ها به‌وفور یافت می‌شوند و افراد در بیشتر مواقع به استفاده از این وسایل ملزم هستند؛ غافل از اینکه در کنار امکانات فراوانی که این دستگاه‌ها برای ما فراهم می‌کنند، به دلیل نوع فناوری به‌کاررفته در آنها ممکن است باعث نقص حریم خصوصی امنیت ما گردند؛ برای نمونه، امروزه تلویزیون‌های هوشمندی وجود دارند که اتصال به اینترنت و داشتن دوربین جزو امکانات ویژه آنهاست، ولی همین ابزار کاربردی و قدرتمند می‌تواند وسیله خوبی برای جاسوسی از منازل و محیط‌ها باشد. نمونه دیگر، گوشی‌های تلفن همراه هوشمند است که به ادعای خود سازندگان، حتی در صورت خاموش‌بودن امکان ردیابی، شنود و جاسوسی در آنها وجود دارد.

به اعتقاد هکرها نفوذ آنها به سیستم‌ها به‌منظور پی‌بردن به سوء استفاده‌هایی است که برخی از افراد، شرکت‌های خصوصی و دولت‌ها از اطلاعات مردم می‌کنند. طبق این استدلال، هکرها می‌خواهند با نفوذ به سیستم‌ها و شفاف‌سازی جلوی سوء استفاده برخی قدرت‌ها را از اطلاعات خصوصی مردم بگیرند و از دید خودشان شرایط خوفناک حاکم بر جامعه را اصلاح کنند. در واقع از نظر آنها، هدف وسیله را توجیه می‌کند. مطابق این

1. http://www.online-literature.com/orwell/1984/.

استدلال، هکرها حفاظت‌کننـده هسـتند، نـه مجـرم (Ethical Hacking: Student Guid, 2000: 133; Baird, 1987: 5). به دلیـل شـباهتی کـه ایـن اسـتدلال بـه رمـان ۱۹۸۴ دارد، بـه ایـن اسـتدلال، استدلال «برادر بزرگ» نیز می‌گویند.

اشکالات استدلال محافظان اجتماعی

بر این استدلال نیز اشکال‌هایی وارد شده؛ از جمله اینکه:

بی‌شک برخی سوء استفاده‌ها از داده‌های شخصی افـراد از سـوی شـرکت‌ها و دولت‌هـا صورت می‌گیرد و چه‌بسا استفاده روزافزون از رایانه‌ها و شبکه‌ها بـرای ذخیـره اطلاعـات بـه سوء استفاده‌های بیشتری نیز بینجامـد. حـال، مشـخص نیسـت کـه آیـا نفـوذ هکرهـا بـه ایـن سیستم‌ها می‌تواند جلوی این‌گونه سوء استفاده‌ها را بگیرد یا نه؟ (Spafford, 1992: 8).

به گفته هکرها آژانس‌های دولتی و سـازمان‌های بـزرگ از طریـق نگهـداری اطلاعـات افراد، حق آنها را برای حفظ حریم خصوصـی خـود نقـض می‌کننـد. سـازمان‌های دولتـی و مؤسسه‌ها برای نگهداری حجم بالایی از اطلاعات افراد بـه رایانـه‌های مرکـزی بزرگـی نیـاز دارند. هکرها بیم این را دارند که جمع‌آوری و نگهداری متمرکز این حجم از داده‌هـا بـرای شناسایی، نظارت و حتی کنترل اعضای جامعه به کار گرفته شود.

هکرها نگرانند که اطلاعات مورد نیاز برای نظـارت و کنتـرل اعضـای جامعـه بـه‌راحتـی قابل دسترسی است. آنها بیان می‌کنند که اطلاعات تلفـن بیشـتر دوسـتان فـرد و روابـط او را نشـان می‌دهنـد و یـا اطلاعـات کارت‌هـای اعتبـاری و حسـاب‌های بـانکی، می‌تواننـد نشـانِ فعالیت‌های تجاری افراد باشند. هکرها تأکید می‌کنند که دولت‌هـا و سـازمان‌های بـزرگ از این اطلاعات برای شناسایی مخالفان بالقوه، نظارت بر فعالیت‌ها، شناسایی ضعف‌ها و کنتـرل افراد بهره می‌گیرند (Baired, 1987: 5,6). آنها می‌خواهند با نفوذهای خود این سوءاسـتفاده‌ها را به صورت شفاف نمایان کنند. به‌طبع این منطقی نیست که بـه دلیـل بـالابردن سـطح آگـاهی افراد، از فعالیت‌های مجرمانه هکرهـا چشم‌پوشـی کـرد. حفاظـت از داده‌هـا و جلـوگیری از سوء استفاده افراد از آنها وظیفه کارشناسان امنیتی فناوری اطلاعات و مجریان قـانون اسـت، نه هکرهایی که اعمال آنها خلاف قانون بوده و فقط با ادعای شفاف‌سازی اعمـالی مرتکـب می‌شوند که از لحاظ اخلاقی نادرست است.

اشکال دیگر به این استدلال آن است که بگوییم هدف وسیله را توجیه نمی‌کند، بلکه افزون بر هدف خوب و مناسب، وسیله نیز فی‌نفسه باید خوب باشد؛ برای مثال، همه ما به طریقی ماجرای رابین‌هود را شنیده‌ایم. رابین‌هود از ثروتمندان و شاه زمان خودش می‌دزدید و به فقیران و نیازمندان می‌بخشید. او کارش را درست می‌دانست، با این استدلال که ثروت زیاد اغنیا و شاه به‌دلیل دزدی‌ها و مالیات‌های زیادی است که با ظلم از مردم نیازمند گرفته‌اند و دزدی او تنها به دلیل کمک به فقیران و نیازمندان جامعه است.

در واقع هدف رابین‌هود گرفتن حق مظلوم از ظالم بود. درست است که هدف رابین‌هود هدفی خوب بوده، ولی او از ابزار مناسبی برای رسیدن به هدفش استفاده نکرده است. با این اوصاف، آیا دزدی از دزد به لحاظ اخلاقی درست است؟ به‌یقین خود عمل دزدی نادرست است و دزدی همواره دزدی محسوب می‌شود و به دلیل اینکه فعل نادرستی است، در نگاه نخست همیشه مردود است. درست است که در نگاه نخست باید در مقابل ظلم و ظالم ایستاد و از حق مظلومان دفاع کرد، ولی اما نه به هر قیمتی. رفتار نادرست را با رفتار نادرست دیگری نمی‌توان اصلاح کرد. به بیان دیگر، برای جلوگیری از جرم نمی‌توان جرم دیگری را مرتکب شد، مگر در مواردی که میان احکام اخلاقی تعارضی موجود باشد و برای مثال برای جلوگیری از قتل یک مؤمن بی‌گناه، مرتکب دروغ شد. چه‌بسا برخی ماجراهایی مانند رابین‌هود را نیز از همین سنخ بپندارند. البته تعارض میان احکام اخلاقی موضوع دامنه‌داری است که در این مقاله فرصت پرداختن به آن نیست.

استدلال پنجم: استدلال هکر دانشجو

برخی از هکرها ادعا می‌کنند که آنها هیچ آسیبی نمی‌رسانند و هیچ چیزی را تغییر نمی‌دهند، بلکه تنها در حال یادگیری چگونگی عملکرد سیستم‌ها و شبکه‌های رایانه‌ای هستند. آنها استدلال می‌کنند که به دلیل گرانی قیمت رایانه‌ها و تجهیزات آنها و ناتوانی مالی دانشجویان در تهیه انواع سیستم‌های رایانه‌ای و تجهیزات شبکه، آنها می‌خواهند تحصیلات خود را با کمترین هزینه پیش ببرند و از همین‌رو، به سیستم‌های دیگران نفوذ می‌کنند. مطابق این استدلال برخی از نویسندگان ویروس‌های رایانه‌ای ادعا می‌کنند که برنامه مخربی که آنها نوشته‌اند، تنها به جهت یادگیری چگونگی نوشتن برنامه‌های رایانه‌ای پیچیده است (Spafford, 1992: 7,8).

اشکالات استدلال هکر دانشجو

اشکالات زیادی به این استدلال وارد است:

اول اینکه می‌دانیم نگاشتن یک برنامه مخرب و یا نفوذ به یک رایانه و جست‌وجو در فایل‌های آن تقریباً هیچ ربطی به آموزش رایانه ندارد. آموزش مناسب در علوم رایانه و مهندسی شامل کشف عمیق در جنبه‌های اساسی نظریه، انتزاع و تکنیک‌های طراحی است که این مهارت‌ها را می‌توان در محیط‌های آزمایشگاهی دانشگاه‌ها به دست آورد. نفوذ به یک سیستم و جست‌وجو در داخل آن سبب بالارفتن دانش تخصصی فرد در زمینه رایانه نمی‌شود.

نوشتن یک برنامه ویروس یا کرم رایانه‌ای و انتشار آن در یک محیط هیچ‌گونه تجربه آموزشی مناسبی را برای دانشجویان فراهم نمی‌کند. همان‌گونه که سرقت خودرو و لذت‌بردن از سواری با آن برای یک مهندس مکانیک فضای آموزشی فراهم نمی‌کند (ibid.). اگر به‌واقع هدف یادگیری در مورد چگونگی کارکرد سیستم‌ها و سخت‌افزارهاست و دانشجویان توانایی مالی برای دسترسی فیزیکی به سیستم‌ها را ندارند، می‌توانند از سیستم‌های مجازی و نرم‌افزارهایی بهره گیرند که قابلیت شبیه‌سازی انواع مختلف سخت‌افزار را دارند. به این ترتیب، بدون پرداخت هزینه زیاد می‌توانند چگونگی عملکرد سیستم‌ها را بررسی کنند، بدون اینکه مشکلی برای سیستم دیگران ایجاد کنند.

افزون‌براین، افرادی که در حال یادگیری چگونگی عملکرد سیستم‌ها هستند، نمی‌دانند که نفوذ آنها چه پی‌آمدهایی را برای سیستم طرف مقابل ایجاد می‌کند (Spafford, 1992: 8). نفوذ به سیستم‌ها و انتشار ویروس‌های رایانه‌ای در اغلب موارد موجب آسیب‌دیدن رایانه‌ها و تحمیل هزینه فراوان برای صاحبان آنها می‌گردد. این نفوذها در بسیاری از مواقع عملکرد سیستم را مختل می‌کنند و در مواردی که رایانه‌های مورد نظر سیستم‌های حساسی مانند سیستم‌های پزشکی، کنترل کارخانه، سیستم‌های مالی و یا سیستم‌های دفاعی باشند، می‌تواند پی‌آمدهای بسیار جدی‌تر و خطرناک‌تری را در پی داشته باشد که هیچ ربطی به آموزش ندارد، و بی‌گمان نمی‌تواند بی‌ضرر در نظر گرفته شود.

تصور کنید اگر این رفتار تحصیلی رواج یابد، در نتیجه ما باید تمام زمان خود را برای

بررسی صحت سیستم‌های خودمان بگذاریم و هرگز نمی‌توانیم به طور کامل به نتایج سیستم‌هایمان اعتماد کنیم. به‌یقین ما حق نداریم به بهانه آموزش به سیستم‌های دیگران نفوذ کرده و برای آنها مشکلات مالی و امنیتی درست کنیم. بنابراین، این استدلال نیز درست به نظر نمی‌رسد.

نتیجه‌گیری

استفاده از رایانه‌ها و اتصال آنها از طریق شبکه و اینترنت فضای مناسبی را برای نفوذ هکرها و دسترسی آنها به اطلاعات فراهم کرده است. این واقعیت که هکرها از یک سو نفوذهای خود را به سیستم‌ها از لحاظ اخلاقی درست می‌دانند و از سوی دیگر، احتمال دستگیر شدن‌شان را ضعیف می‌پندارند، به آنها این جرئت و جسارت داده می‌شود که در ماجراجویی‌های اینترنتی خود ریسک کنند.

هکرها براساس نیت و شیوه عملکردشان به سه دسته کلاه‌سفید، کلاه‌سیاه و کلاه‌خاکستری تقسیم می‌شوند. نفوذ هکرهای کلاه‌سفید به دلیل اینکه هدفشان ارتقای امنیت سازمان‌هاست و با مجوز رسمی کار خود را انجام می‌دهند، به لحاظ اخلاقی درست است، اما نفوذ هکرهای کلاه‌سیاه به دلیل اینکه نیت سوء دارند و نیز نفوذهایشان به سیستم‌ها و اطلاعات درون آنها آسیب می‌رساند به لحاظ اخلاقی نادرست است.

هکرهای کلاه‌خاکستری از بیرون سازمان و با هدف افشای نقاط ضعف امنیتی سیستم‌ها و امن‌کردن آنها به رایانه‌ها و شبکه‌های سازمان‌ها نفوذ می‌کنند. این هکرها کار خود را از نظر اخلاقی درست می‌دانند، چون به گفته خودشان نیت آنها امن‌کردن سیستم‌ها و کمک به ارتقای امنیتی سازمان‌هاست، ولی از آنجا که نفوذ به یک سیستم پی‌آمدهای پیدا و پنهان کوتاه مدت و بلند مدت بسیاری را در پی دارد که شناسایی این پی‌آمدها به‌سادگی امکان‌پذیر نیست، پس نمی‌توان گفت که نفوذ هکرهای کلاه‌خاکستری هیچ آسیبی به سیستم‌ها و جامعه نمی‌رساند.

هکرهای کلاه‌خاکستری برای توجیه اخلاقی نفوذهایشان استدلال‌هایی اقامه کرده‌اند که در این مقاله به بررسی و نقد برخی از مهم‌ترین استدلال‌های آنها (آزادی اطلاعات،

استدلال امنیتی، سیستم‌های بلااستفاده، محافظان اجتماعی و هکر دانشجو) پرداختیم. خلاصه اینکه همان‌گونه که گذشت اخلاقی‌بودن هر کاری افزون بر حسن فاعلی، نیازمند حسن فعلی نیز هست و هرچند هکرهای کلاه‌خاکستری ادعا می‌کنند که نیت آنها خوب است، رفتارشان یعنی نفوذ به سیستم‌ها، بدون اجازه صاحبان آنها به‌خودی‌خود غیراخلاقی است. بنابراین، نفوذ هکرهای کلاه‌خاکستری به لحاظ اخلاقی نادرست است.

کتابنامه

1. “2015 Costs of Cyber Crime Study: United States,” http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report, Hewlett Packard Enterprise, October, 2015.
2. Baird, Bruce J; Baird Jr, Lindsay L; Ranauro, Ronald P. (1987), “The moral cracker”, *Computers & Security*, Vol 6, Issue 6, 471 - 478.
3. Brey, Philip (2007), *Ethical Aspects of Information Security and Privacy*, *Security, Privacy, and Trust in Modern Data Management*, New York: Springer Berlin Heidelberg.
4. Denning, Dorothy E. (1990), “Concerning Hackers Who Break into Computer Systems,” 13th National Computer Security Conference, Washington, D.C, Oct. 1-4.
5. Ethical hacking, Student Guide, Internet Security Systems, Inc., 2000.
6. Falk, Courtney (2004), “Gray Hat Hacking Morally Black And White”, Cyber Security Group (CSG), Training Conference.
7. Fötinger, Christian S. (2004), Ziegler, Wolfgang; Understanding a hacker’s mind – A psychological insight into the hijacking of identities, Krems, Austria: Donau-University Krems.
8. Graves, Kimberly (2010), *CEH: Certified Ethical Hacker Study Guide*, Indiana: Wiley Publishing, Inc.
9. Himma, Ken (2005), “Information and Intellectual Property Protection: Evaluating the Claim that Information Should be Free”, *APA Newsletter on Philosophy and Law*, 4, 3–9.

10. Himma, Kenneth Einar (2007), *Internet security: hacking, counterhacking, and Society, United States of America*: Jones & Bartlett Publishers, Inc.
11. Himma, Kenneth Einar Tavani, Herman T. (2008), *The handbook of computer ethic*, Canada: John Wiley & Sons, Inc.
12. http://www.ashiyane.ir/archive.php?id=2
13. http://www.online-literature.com/orwell/1984/
14. http://www.usatoday.com/story/news/nation/2015/08/06/russia-reportedly-hacks-pentagon-email-system/31228625/
15. Jennings, Richard C. (2010), "Professional Practice & Ethics", *Computer Science Tripos Part IA*, Department of History and Philosophy of Science University of Cambridge.
16. Levy, Steven (1994), *Hackers Heroes of the Computer Revolution*, New York: Dell Publishing a division of Bantam Doubleday Dell Publishing Group.
17. Martin, Mike W. (2005), *Schinzinger, Roland; Ethics in Engineering*, Fourth Edition, Mc-Graw Hill.
18. Spafford, Eugene H. (1992), "Are computer break-ins ethical?" Journal of Systems Software, 17.
19. Stallman, Richard M. (1992), "Against User Interface Copyright," 92 Proceedings of the conference on TRI-Ada.
20. Tavani, Herman T. (2004), *Ethics and Technology: Ethical Issues in an Age of information and Communication Technology*, New York: John Wiley & Sons, Inc.
21. Young, Susan; Aitel, Dave (2004), *the hackers handbook: The Strategy behind Breaking into and Defending Networks*, United States of America: Auerbach Publications.
۲۲. سعیدی، سینا، حجت اله حاجی‌حسینی و صبا سعیدی (۱۳۹۲)، «بررسی عوامل مؤثر بر نقض قانون حق نشر توسط کاربران اینترنت»، *اخلاق در علوم و فنّاوری*، سال هشتم، ش۲.