Punishing Internet hackers

Government officials should harness Parsons' talents to benefit society

MICHAEL WARD

The New York Times reported last week that authorities arrested an 18-year-old Minnesota teen for "intentionally causing damage to a protected computer." Because of this, Jeffrey Lee Parsons, or "teekid" — his Internet name — could face a $250,000 fine and up to 10 years in prison.

Federal officials could imprison him and few Americans would care, but that would be a waste of talent.

"Cyber hacking is not joy riding," said Attorney General John Ashcroft. "Hacking disrupts lives and victimizes innocent people across the nation."

Indeed it does.

The variant of the virus for which Parsons is supposedly responsible corrupted more than 500,000 computers worldwide and cost U.S. citizens $1.3 billion, according to The New York Times.

The Washington Post reports that "teekid" felt little remorse for his exploits. His personal Web site — recently taken offline — allowed users to download his viruses and augment them. "My little p2p worm spreads via Kazaa and iMesh, downloads a file from the Web," Parsons said in reference to one of his earlier creations. "No biggie."

Obviously, this is not the work of a saint. Certainly Parsons is a troublemaker, one whom no one should seek to emulate. However, given his age and present situation, his indisputable talent should be harnessed.

"My belief is that hacking, above all ... is about the passion and obsession for knowledge and truth," said Richard Thieme at last year's Def Con, a famous hacker convention. Modern Dr. Frankensteins, Parsons and his colleagues worldwide think first about testing their limits and last about the consequences.

Parson's is simply the latest in a short list of infamous hackers.

Kevin Mitnick was on the lam for five years before being apprehended. To this day, his actual crimes pale in comparison to the legends shrouding his personality. Among other supposed exploits, Mitnick is believed to be the inspiration for the 1983 movie "War Games" – a film in which a young Matthew Broderick plays a teenage genius who is able to hack into the Pentagon to start a third World War, according to the San Francisco Chronicle.

Kevin Poulsen, similarly, achieved fame when in 1990, he won a 944 Porsche from the L.A. radio station KISS FM. Of course, he won it by hacking Pacific Bell's switching system, assuring him he would be the 102nd caller to the station, but he was the winning caller nonetheless.

After spending time in prison, these men are leading successful lives as computer security and Internet specialists.

Enter Jeffrey Lee Parsons.

According to the FBI's Web site, the agency is only accepting applications for "Special Agent" from those with experience in specific disciplines. One of these is computer science. The CIA is looking for the same.

Given the fact that, at age 18, Parsons supposedly has been able to hack into the government of Minnesota and mutate a virus that infected much of the United States, it seems as though he might have the background the government is looking for.

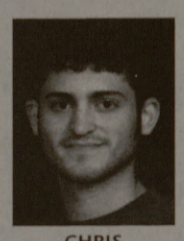
True, if found guilty, he would be a criminal, but that would only make his employment cheaper for the government. One can reasonably give Parsons the benefit of the doubt and blame his immaturity and the "teen angst" he might harbor as definite catalysts for his hacking. Equally as reasonable is the notion that the government should give Parsons the opportunity to work for free — under house arrest — for the length of whatever jail sentence he would have received.

To let his talent rot and his teenage-fueled resentment build behind bars would be dangerous.

While Parsons may not be a genius hacker — after all, he advertised his exploits on his own Web site — he's someone whom government agencies could mold into a successful computer systems engineer. Considering that government agencies are only able to compensate their employees a fraction of what a commensurate job opportunity would offer in the private sector, applicants in certain disciplines are hard to come by. If the competitive, cutthroat industry of computer technology can trust former hackers such as Kevin Mitnick and Kevin Poulsen, surely the FBI or some similar government entity can trust and cultivate the talent of a young hacker.

Michael Ward is a senior history major.

Hacker activities are serious crimes that deserve harsh punishments



CHRIS LIVELY

FBI officials have found and apprehended the man responsible for perpetrating a large part of the latest worldwide computer attack. According to CNN, 18-year-old Jeffrey Lee Parsons was arrested Aug. 29 in Hopkins, Minn., on a federal charge of "intentionally causing or attempting to cause damage to a computer." Parsons took an already active computer worm, known as the "blaster" worm, modified it, and derived a version called "Blaster.B."

The blaster worm's primary goal is reaching as many PCs as possible, and it spreads at the speed of the Internet. It attacks computers that run Microsoft Windows and can have devastating effects on systems, corporations and individuals. In the latest outbreak of "blaster" attacks, nearly 500,000 computers worldwide were affected beginning on Aug. 11. The attack disrupted commerce and caused $1.3 billion in damage, according to The New York Times. Parsons' version infected more than 7,000 computers.

Pending trial and conviction, Parsons could face up to 10 years in prison and a $250,000 fine, according to The Washington Post. Many feel that technological criminals such as Parsons are a rare breed of gifted geniuses who should be allowed to utilize their talents for government agencies. The reality is, however, that computer hackers are more of a threat to society than just about any other sort of criminal and should be sent to jail.

Hackers such as Parsons retain malevolent and deliberate intentions that can torment the livelihoods of countless numbers of innocent people, as witnessed this past month. Parsons should not be allowed to benefit from his deviant behavior; the Parsons case needs to send the clear and direct message that this type of behavior will not be tolerated.

In today's society, computer criminals seem to be more socially acceptable than other, traditional criminals. However, this statement illustrates a common misconception. Computer crimes are underrated by much of the public in terms of their severity. According to The Washington Post, U.S. Attorney John McKay stated, "With this arrest, we want to deliver a message to cyber-hackers here and around the world. Let there be no mistake about it, cyber-hacking is a crime."

Following the onset of the information age, the tangibility of assets and the like has obviously faded due to the rising usage of computers for business and banking. When a vulnerable computer is attacked by a virus or worm, the ramifications can be much more detrimental than simply having to replace a thousand-dollar machine.

It does not make sense to allow Parsons to work for a government agency when he is the government's worst enemy.

If Parsons was allowed to be employed in a prestigious government position, an example certainly would be set. Granting him this sort of opportunity would not deter future hackers from initiating this sort of behavior and would, if anything, reinforce it.

Many government agencies such as the CIA highly value the skills Parsons possesses. He may also be more highly skilled than most others with similar abilities, but it is because he has been practicing an illegal activity that should not be performed by anyone but a government agent. If the CIA needs a sharpshooter, it would not hire the Washington, D.C., sniper to do the job.

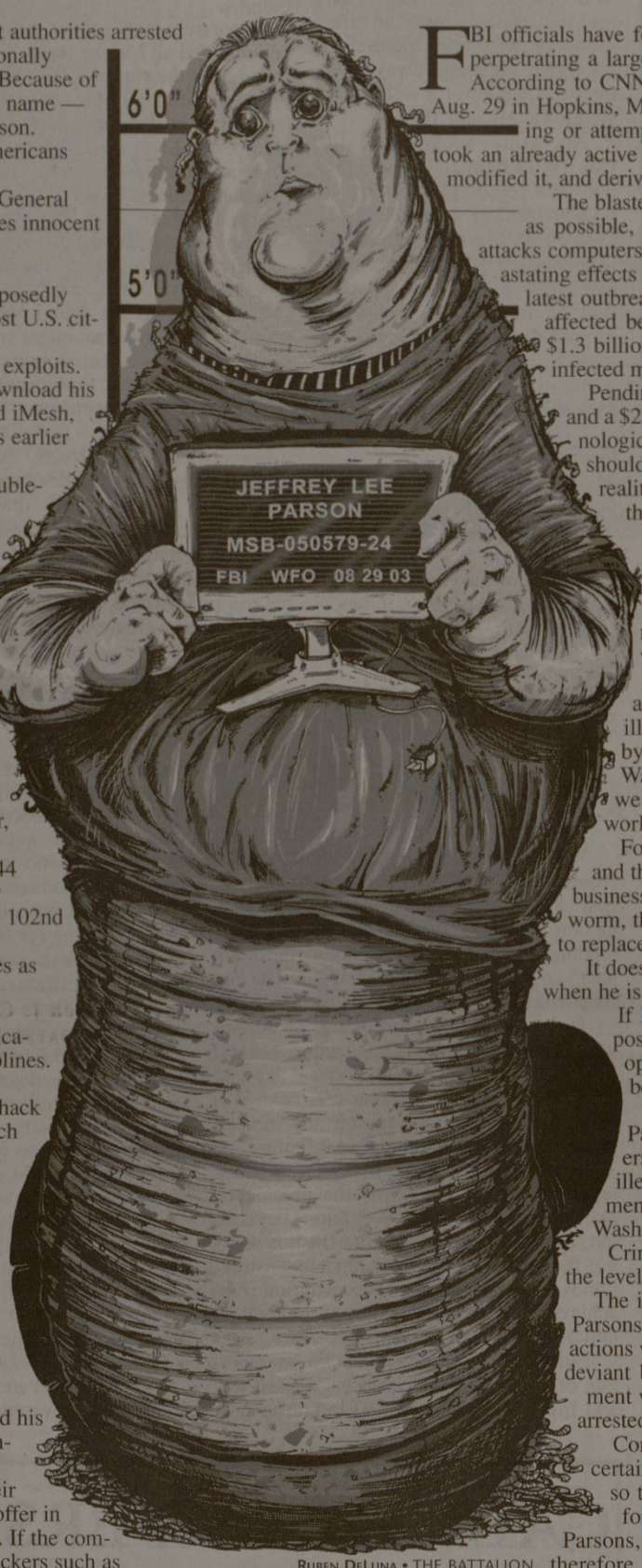
Criminal behavior should be treated as criminal behavior, regardless of the level of talent involved.

The immediate threat of computer crimes is evident and as real as ever. Parsons made a wrong decision, a path chosen that cannot be tolerated. His actions were not negligent, but intentional and spiteful. Similar to any other deviant behavior, Parsons' actions should not be reinforced with employment where he would continue utilizing the knowledge and skills he was arrested for.

Computer crime is a relatively new occurrence. One thing that is for certain is that as technology continues expanding at an exponential rate, so too will the prevalence of computer-related crime. Now is the time for an example to be set.

Parsons, an intelligent adult, knowingly committed a serious crime, and is therefore a serious criminal. His capabilities, just as with the majority of computer criminals, are of no significant advantage to society. Hence, Parsons and other hackers, regardless of their ages or other attributes, should be excluded from government employment.

Chris Lively is a senior sociology major.



RUBEN DELUNA • THE BATTALION

MAIL CALL

Protesters not all violent

In response to Matt Rigney's Sept. 8 column:

Day after day peaceful protesters line the sidewalk outside of Planned Parenthood's controversial abortion clinic in Bryan. The Bryan-College Station Eagle reported that "the clinic in Bryan also is distinguished among the 800 or so owned by Planned Parenthood for having arguably the most consistent and active protester presence," and Texas Monthly magazine stated: "seven days a week, 10 hours a day, picketers line the sidewalk, trying to change hearts and minds."

It was disappointing that Mr. Rigney's editorial appeared to portray all pro-life people as violent. The people of faith who are taking a peaceful stand against abortion outside of Planned Parenthood's facility in Bryan are actually the ones who are working to end the brutal violence that has plagued Aggieland for far too long.

David Bereit '90
Executive Director
Brazos Coalition for Life

Stopping hate crimes in the U.S.

JOHN DAVID BLAKLEY

The Local Law Enforcement Enhancement Act was introduced into the Senate in May 2003 as a means of providing federal assistance to state and local jurisdictions to prosecute hate crimes. Hate crime legislation is not new to Capitol Hill, but this bill proposes to extend federal protection to hate crimes that are based on sexual orientation, which has never been included in a hate crimes law, gender and disability. This legislation is necessary to ensure protection to those who experience discriminate violence and must be passed.

Many consider the inclusion of crimes based on a person's sexual orientation to be the most necessary section of the bill, as the gay, lesbian and bisexual community has increasingly become victims of hate crimes.

According to the FBI, reported hate crimes based on sexual orientation have tripled since 1991. Hate crimes by definition include exclusively crimes which involve violence, and includes no prohibitions against speech, expression or association, according to the bill.

The Human Rights Campaign, the largest lesbian and gay political organization in the country, provides one example of the necessity for expansion of hate crime legislation. According to HRC, on Feb. 22, 2001, Kyle Skyock, a 16-year-old high school student, was beaten unconscious by four other teens and left for dead. After the incident, one of the perpetrators reportedly told others that he had beaten a "fag."

Skyock's injuries included a fractured skull, burn blisters, a black eye, three broken ribs and a bruise on his stomach in the shape of a two-by-four, according to the Rocky Mountain News. Despite the severe injuries he suffered, local police refused to interview Skyock for six months following the attack. The police justified its action by saying Skyock was drunk and fell. A crime this violent, blatantly motivated by hate of the gay community, deserves a much more eager response from local police.

> *"Hate crimes are assaults on the principles of freedom and equality that make America great."*

The law enforcement enhancement act can in many ways eliminate the consistent flaws seen in the prosecutions of hate crimes by state and local officials, such as those found in Skyock's case. In the introduction of the act to the Senate, Sen. Edward Kennedy called the bill "an appropriate back up for state and local law enforcement, to deal with hate crimes in cases that would not otherwise be effectively investigated and prosecuted."

Under the enhancement act, state and local government will retain their primary roles in responding to violent crimes, but the act will allow the use of federal resources and expertise in the identification and proving of hate crimes.

Whether legislators approve of the practice of homosexuality should not affect their vote on the enhancement act. What this act stands for is the idea that nowhere in the United States will violence toward a person or people, based on their sexual preference, gender or disability be allowed without a proper response.

The effects of hate crimes ripple beyond the injuries suffered by individual victims. These acts are committed solely to frighten and intimidate a certain group of people. According to the findings of the U.S. Senate Committee on the Judiciary, violence motivated by personal characteristics such as sexual orientation disrupts the tranquility and safety of communities and is deeply divisive.

Hate crimes are assaults on the principles of freedom and equality that make America great. The Local Law Enforcement Enhancement Act has the potential to provide a proper response to these intolerable deeds.

John David Blakley is a sophomore political science major.