

## Digital La Cosa Nostra: The Computer Fraud and Abuse Act's Failure to Punish and Deter Organized Crime

"If one teenager can jeopardize over a hundred Web sites from his parent's house, imagine what groups of seasoned cybergangs can do."<sup>1</sup>

United States Secret Service agents sat in an unmarked building poised to begin their raid.<sup>2</sup> The agents spent months planning and organizing the raid, designed in order to take down a gang that had robbed, threatened, and terrorized people every day for over two years.<sup>3</sup> At approximately nine o'clock at night the Secret Service Agents, armed with pistols and semi-automatic machine guns, received the order allowing them to take down the suspects.<sup>4</sup> The agents were aware that some of the suspects may have stockpiled weapons.<sup>5</sup> Most of the suspects were still in their homes when the agents moved in.<sup>6</sup> Dubbed "Operation Firewall," the raid resulted in the arrest of twenty-eight individuals.<sup>7</sup>

Operation Firewall was not a raid on drug dealers or traditional organized crime, but instead was an effort to take down organized cybercrime<sup>8</sup> in the shape of a newly-formed cybergang.<sup>9</sup> Known as "Shadowcrew" to their world-wide members and the law enforcement agents sent to apprehend them, the cybergang had committed identity theft,

---

1. Tom Spring, *Web of Crime: Who's Catching the Cybercrooks?*, PCWORLD, Aug. 29, 2005, <http://www.pcworld.com/printable/article/id,122245/printable.html> (quoting Timothy Nestor, an FBI investigator directly involved with the new FBI cyber task force).

2. Brian Grow & Jason Busch, *Hacker Hunters: An Elite Force Takes on the Dark Side of Computing*, BUSINESS WEEK, May 30, 2005, at 74, available at 2005 WLNR 8340607.

3. *Id.*

4. *Id.*

5. *Id.*

6. *Id.*

7. TECHWEB TECHNOLOGY NEWS, *Secret Service Busts Cyber Gangs*, Oct. 29, 2004, <http://www.techweb.com/wire/51201522>, available at 2004 WLNR 14267486.

8. See Grow & Busch, *supra* note 2.

9. TECHWEB TECHNOLOGY NEWS, *supra* note 7.

robbery, extortion, and a variety of other crimes.<sup>10</sup> The gang members that composed Shadowcrew were suspected of stealing and reselling millions of dollars' worth of stolen credit card numbers and personal identification documents.<sup>11</sup> This Note will address the problems created by cybergangs and the methods necessary to combat cybercrime.

The Computer Fraud and Abuse Act (CFAA) was enacted in order to provide the government with a means to punish computer criminals.<sup>12</sup> The CFAA fails to address the threat posed by cybergangs because it does not take into account the distinct problems that organized cybercrime presents. Therefore, the Racketeer Influenced Corrupt Organizations Act (RICO) should be used to prosecute cybergangs and their members.<sup>13</sup> This Note will discuss the growing crisis of cybergangs and the prosecutorial methods necessary to stop them before they become an overwhelming problem. Section I of this Note includes a brief introduction to cybercrime with classifications that will help explain why cybergangs are more dangerous than common cybercriminals.<sup>14</sup>

Section II will define what cybergangs are and how they are formed. The analysis will also explore computer criminals' rationale in forming cybergangs. This Note will continue with an explanation of the common schemes that many cybergangs employ to carry out their goals. The federal prosecution of Shadowcrew members will be examined in order to demonstrate that current prosecutorial methods are failing. Further, a comparison between the structures of cybergangs and the Mafia will show that the methods of prosecuting organized crime could be successful in prosecuting cybergangs.

Section III will address Congress's response to cybercrime. The CFAA, as previously mentioned, is the main statute used in prosecuting criminals in the growing area of cybercrime.<sup>15</sup> Punishment under the CFAA will be examined to show that the Act does not effectively punish cybergangs. Various cases prosecuted under the CFAA will be analyzed to examine flaws in the statute that members of a cybergang may exploit. Weaknesses in the classification of cybercrime will also be discussed.

Section IV will examine whether cybergangs should be prosecuted under

---

10. Grow & Busch, *supra* note 2.

11. *Id.*

12. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000 & Supp. 2003).

13. Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961 to 1968 (2000 & Supp. 2003).

14. See Douglas Thomas & Brian D. Loader, *Introduction to CYBERCRIME: LAW ENFORCEMENT, SECURITY AND SURVEILLANCE IN THE INFORMATION AGE 2-3* (Douglas Thomas & Brian D. Loader eds., Routledge 2000).

15. See Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000 & Supp. 2003).

a statute similar to RICO.<sup>16</sup> The similarity of cybergangs to organized crime indicates that the harsh penalties prescribed under RICO will have a similar effect on the prosecution of cybercrime. RICO is believed to have slowed the progression of the Mafia and, therefore, RICO should be used to proactively attack cybergangs before they become as widespread as the Mafia.

## I. CYBERCRIME

A broad definition regards cybercrime as “computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks.”<sup>17</sup> Cybercrime has often been divided into three recognizable categories: 1) crimes in which the computer is the actual target of the crime; 2) crimes in which the computer is used merely as a tool to commit other crimes, such as fraud and extortion; and 3) crimes in which use of a computer is only an incidental aspect of the commission of the crime, such as when a computer is used for purposes of child pornography or other means of communicating illegally.<sup>18</sup> The crimes that this Note will discuss are crimes where a computer is the target and crimes where the computer is used as an instrument to commit the crime. Just as there are classifications of cybercrime, there are also different classifications of cybercriminals. There are three categories of computer criminals on the Internet: “script-kiddies,” “hackers,” and “crackers.”<sup>19</sup>

### A. Classification of Criminals

#### 1. Script-kiddies

The first group, “script-kiddies,” carries out most of the nuisance-crime that takes place on the Internet.<sup>20</sup> Script-kiddies do not possess the knowledge that would allow them to undertake more damaging work and

---

16. Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961 to 1968 (2000 & Supp. 2003).

17. CYBERCRIME, *supra* note 14, at 3 (mentioning the difficulties in fully describing and encompassing every aspect of cybercrime).

18. Susan W. Brenner, *Defining Cybercrime: A Review of State and Federal Law*, in CYBERCRIME: THE INVESTIGATION, PROSECUTION AND DEFENSE OF A COMPUTER-RELATED CRIME 12-16 (Ralph D. Clifford ed., Carolina Academic Press 2001).

19. Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 918 (2003).

20. *Id.*

are limited to exploiting common security weaknesses.<sup>21</sup> The majority of script-kiddies can only affect small changes in security programs, and their programming mistakes frequently cause the damage inflicted upon a website or security center.<sup>22</sup> Script-kiddies, unlike other computer criminals, are not seeking financial gain through their security breaches.<sup>23</sup> Still, script-kiddies should not be dismissed easily because these criminals frequently develop into more sophisticated hackers and crackers.<sup>24</sup>

## 2. Hackers

The next group of cybercriminals is known as “hackers,” the most recognized Internet criminals.<sup>25</sup> A hacker is alleged to be driven by curiosity to determine how computer systems work and to learn the intricacies of security systems.<sup>26</sup> Notoriety and the ability to boast about the hack are the major motivations for a hacker to intrude upon computer systems.<sup>27</sup> Hacking into computer systems requires a thorough understanding of the system, and many hackers find this information to be interesting.<sup>28</sup> A computer criminal labeled as a hacker has the ability to use standard hacking programs freely available on the Internet with much more sophistication than script-kiddies.<sup>29</sup> Hackers should not be taken lightly as they cause a great deal of damage to computer systems in their quest for knowledge and information.<sup>30</sup> Hackers, however, are not as dangerous as the following cybercriminals: “crackers.”

---

21. *Id.*

22. *Id.*

23. MCAFEE, INC., MCAFEE VIRTUAL CRIMINOLOGY REPORT: NORTH AMERICAN STUDY INTO ORGANIZED CRIME AND THE INTERNET 10 (July 2005), [http://www.mcafee.com/us/local\\_content/misc/mcafee\\_na\\_virtual\\_criminology\\_report.pdf](http://www.mcafee.com/us/local_content/misc/mcafee_na_virtual_criminology_report.pdf). McAfee is an Internet security company that is best known for antivirus software.

24. Skibell, *supra* note 19, at 919.

25. Philip W. Esbenschade, *Hacking: Juveniles and Undeterred Recreational Cybercrime*, 23 J. JUV. L. 52, 54 (2002-03).

26. *Id.*

27. Skibell, *supra* note 19, at 919-20.

28. RICHARD POWER, TANGLED WEB: TALES OF DIGITAL CRIME FROM THE SHADOWS OF CYBERSPACE 10-13 (Que Corp. 2000) (interview with Sarah Gordon of IBM’s Thomas J. Watson Research Center describing common factors that appeared among many of the individuals who were labeled hackers, including the search for knowledge and information).

29. Skibell, *supra* note 19, at 919.

30. See BERNADETTE H. SCHELL & JOHN L. DODGE WITH STEVE S. MOUTSATSOS, THE HACKING OF AMERICA: WHO’S DOING IT, WHY, AND HOW 18 (Quorum Books 2002) (stating that Kevin Mitnick, a criminally prosecuted hacker who alleges that he is not a criminal, invaded thirty-five major corporations causing \$300 million in damages).

### 3. Crackers

“Crackers” are the group of cybercriminals previously thought to be the most dangerous to computer systems.<sup>31</sup> Crackers attack vulnerable computers for personal profit and for malicious criminal purposes.<sup>32</sup> There is a fine line between a hacker and a cracker; the motivation for financial profit or criminal purpose is the only difference between the two groups.<sup>33</sup> Crackers, who seek monetary gain through their crimes, are deemed to be the biggest security risk, but as this Note will prove, crackers should no longer be considered the most dangerous Internet criminals because cybergangs are able to cause far more damage.

## II. CYBERGANGS

### A. Cybergangs Defined

Cybergangs are defined as groups of cybercriminals that have acquired various computer skills and use those skills to move their criminal activities to cyberspace.<sup>34</sup> The solitary rogue hackers who commit crimes for thrills or out of curiosity are being replaced by cybergangs who are not simply curious about computers, but instead use them to commit financially-motivated crimes.<sup>35</sup> In the past, hackers were considered solitary perpetrators of criminal conduct in cyberspace, but with the increased use of the Internet, groups of criminals are banding together.<sup>36</sup> Cybergangs are formed for purely monetary reasons, similar to crackers.<sup>37</sup> Through the use of the Internet, cybergangs are given immediate access to fellow members, allowing them to pool their knowledge and, in turn, inflict greater financial damage on their potential victims.<sup>38</sup>

### B. Formation of Cybergangs in the Context of Shadowcrew

Cybergangs are formed as highly organized criminal groups, similar to

---

31. Skibell, *supra* note 19, at 920.

32. *Id.*

33. Esbenshade, *supra* note 25, at 54.

34. Poonam Khanna, *Cybercrime on the Rise*, COMPUTER DEALER NEWS, Mar. 7, 2005, available at 2005 WLNR 13206037; see MCAFEE, *supra* note 23, at 10.

35. Grow & Busch, *supra* note 2.

36. Khanna, *supra* note 34. “Ten years ago, we were mainly looking at amateurs, and now we’re looking at professionals.” *Id.* (quoting James Lewis, a senior fellow and director of the Technology and Public Policy Program at the Center for Strategic and International Studies in Washington, D.C.).

37. Spring, *supra* note 1.

38. See MCAFEE, *supra* note 23, at 10.

the Mafia, except entirely online.<sup>39</sup> Evidence obtained from Operation Firewall, the raid on members of the cybergang Shadowcrew, provides information about the common structure of cybergangs. Before Shadowcrew was shut down it had approximately 4000 registered members from around the globe.<sup>40</sup> The cybergang worked in a fashion similar to the Mafia by providing the framework and services for criminals to practice in their specialty.<sup>41</sup> Former United States Attorney Scott Christie stated that the business Shadowcrew conducted proves these gangs are “highly structured and very well organized.”<sup>42</sup>

Shadowcrew was organized into different levels of power with the highest level known as “Administrators.”<sup>43</sup> Shadowcrew Administrators were the members that oversaw the gang’s overall business functions and were considered the gang’s enforcers, making sure profits were turned over.<sup>44</sup> Administrators of Shadowcrew also determined which merchandise would be offered for sale and which individuals would be allowed into the gang.<sup>45</sup> Administrators remained outside of the day-to-day activities.<sup>46</sup>

The next level in the hierarchy consists of “Moderators.”<sup>47</sup> The members of the gang who proved their skill through prior criminal activities were allowed to become Moderators.<sup>48</sup> Moderators were in charge of running the forums on Shadowcrew’s website that bought and sold credit card information and other identification documents.<sup>49</sup> The forums on Shadowcrew’s website discussed strategies on stealing credit card numbers, forging bank cards, and creating identification documents, such as driver’s licenses and diplomas in order for the information to be accepted as authentic.<sup>50</sup> At the time of Shadowcrew’s indictment, there were a dozen members that had obtained Moderator status.<sup>51</sup>

“Reviewers” were the next level of criminals in the cybergang.<sup>52</sup>

---

39. See TECHWEB TECHNOLOGY NEWS, *supra* note 7.

40. John McCormick & Deborah Gage, *Shadowcrew: Web Mobs*, BASELINE, Mar. 7, 2005, <http://www.baselinemag.com/article2/0,1540,1774870,00.asp>, available at 2005 WLNR 3987607.

41. *Id.*

42. *Id.*

43. See Grow & Busch, *supra* note 2.

44. *Id.*

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. *Id.*

50. McCormick & Gage, *supra* note 40.

51. *Id.*

52. *Id.*

Reviewers verified the identification documents and credit card information by running tests on stolen credit card numbers.<sup>53</sup> The main process used by a Reviewer to check the validity of credit card information was called a “dump check.”<sup>54</sup> A Reviewer would hack into a company’s cash register system (usually through a backdoor used by security personnel for the company) in order to test whether the card would be accepted when entering nominal dollar amounts and then would issue a report regarding the quality of the credit card information.<sup>55</sup> Once the Reviewer obtained personal identification documents, he would write a review describing the documents, including the thickness of driver’s licenses, presence of holograms on official documents, and whether the document could be passed off as authentic.<sup>56</sup> After the goods were reviewed they were offered for sale on the forums or through an auction site, similar to eBay, on Shadowcrew’s website.<sup>57</sup>

The “Vendors” were the second lowest grouping of Shadowcrew members.<sup>58</sup> Vendors were responsible for the sale of the stolen information, as well as performing other services, such as money laundering.<sup>59</sup> The Vendors were also the members responsible for hacking into a company’s register system, knowledge of which was then passed on to the Reviewers so that they could verify the card information.<sup>60</sup>

The lowest ranking group of cybercriminals was the “General Members” who were responsible for gathering and sharing credit card numbers and instructions on how to obtain and falsify identification documents.<sup>61</sup> Members were also able to prove themselves and their loyalty by working their way up the ranks of the gang.<sup>62</sup> Just like the Mafia, General Members needed a senior member to vouch on their behalf before they were allowed to pitch a new idea or sale suggestion to the Administrators.<sup>63</sup> This organizational structure seems all too familiar to law enforcement officers familiar with investigating the Mafia.

---

53. Grow & Busch, *supra* note 2.

54. McCormick & Gage, *supra* note 40.

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. *Id.*

60. Grow & Busch, *supra* note 2.

61. McCormick & Gage, *supra* note 40. Thousands of members were allowed access to the forums available on the website to share instructions on credit card fraud and identification fraud, but they were not allowed access to sensitive forums which were protected by passwords. *Id.*

62. *Id.*

63. *Id.*

C. Comparison to the Mafia<sup>64</sup>

Cybergangs are structured very similarly to the Mafia, the only real difference being that cybergangs operate entirely online. The structure of cybergangs and the Mafia are similar enough to show that the prosecution methods that worked on the Mafia can work on cybergangs. The structure of a typical Mafia family is well-documented.

The hierarchy of the Mafia was outlined in a report issued to President Ronald Reagan in 1986.<sup>65</sup> The report states that organized criminal groups are carefully structured in order to accomplish a particular function within the organization.<sup>66</sup> Membership within the criminal organization is generally limited to certain traits, such as race, ethnicity, or criminal background.<sup>67</sup> This is very similar to cybergangs in that the members of the cybergang were all collected as prolific or experienced computer hackers, skilled in various aspects of computer crime; the members of each criminal organization obtain a sense of belonging and an opportunity for economic gain.<sup>68</sup>

The top position of an organized crime ring is the “Boss.”<sup>69</sup> The Boss is considered the head of the family and avoids participating in the day-to-day operations of the family.<sup>70</sup> The Boss, however, is rewarded for his prestige by receiving a percentage of the gains from criminal activities taking place.<sup>71</sup> The Boss of a Mafia family is directly comparable to the cybergang members known as Administrators.<sup>72</sup> In a general comparison, these top-ranking members perform the same functions, are rewarded in very similar fashions (as they both receive percentages of the profits from criminal activities), are seen as the figureheads of their groups, and remain outside of the day-to-day activities of the gang while still controlling the

---

64. This section contains a specific comparison to La Cosa Nostra and will use the words “family,” “Mafia,” and related terms in the manner used in the President’s Commission Report cited below.

65. PRESIDENT’S COMM’N ON ORGANIZED CRIME, *THE IMPACT: ORGANIZED CRIME TODAY: REPORT TO THE PRESIDENT AND THE ATTORNEY GENERAL* (1986). The report was created pursuant to Executive Orders 12435 and 12507 and Public Law 98-368, 98 Stat. 490; it is a detailed investigation into the inner workings of organized crime based on years of investigations, informant testimony, and other compiled sources. *Id.* at iii.

66. *Id.* at 26.

67. *Id.* at 27.

68. *Id.*

69. *Id.* at 39.

70. *Id.*

71. *Id.*

72. McCormick & Gage, *supra* note 40 (stating that Administrators are able to remain outside of the day-to-day activities and still receive a cut of the illegal activities that take place below them).

direction in which the gang is moving.

The next highest position in a Mafia family is the “UnderBoss.”<sup>73</sup> The UnderBoss is being groomed to take over for the Boss when the time arises.<sup>74</sup> There is normally one UnderBoss per family.<sup>75</sup> While there is no direct comparison between an UnderBoss and a member of Shadowcrew’s cybergang, the position could easily develop.

The “Capo” or “Captains” are the next highest rank in the Mafia.<sup>76</sup> Once one proves himself to the family as a financial success, he is promoted to the title of Captain where he supervises the day-to-day operations of the family.<sup>77</sup> Captains of a Mafia family are similar to the Moderators of a cybergang. The Moderators oversee the criminal activities of the cybergang just like Captains in the Mafia are in charge of the oversight of criminal activities in a Mafia family.<sup>78</sup> The Captains and the Moderators both prove their worth through their past criminal activities and are trusted to realize their earning potential in the organization.

The lowest formal rank of Mafia members are known as “Soldiers.”<sup>79</sup> The Soldiers of a Mafia family are initiated but are yet unproven as financial contributors.<sup>80</sup> Soldiers are the members who actually commit the crimes on the street.<sup>81</sup> Soldiers are connected to the family but they are not given a full title until they can prove themselves as top contributors.<sup>82</sup> There is no direct comparison available between the members of a cybergang and the Soldiers of a Mafia family.<sup>83</sup>

The largest group of Mafia members, comparable to a cybergang’s General Members, are the “Associates.”<sup>84</sup> Associates do not need to be of any specific ethnicity in order to work for the family, but they are usually connected in some way to a Soldier.<sup>85</sup> In order for an Associate to become a member of the family, he must be vouched for, or sponsored, by an existing member.<sup>86</sup> The sponsor is also the key ingredient for a General

---

73. PRESIDENT’S COMM’N, *supra* note 65, at 39.

74. *Id.*

75. *Id.*

76. *Id.* at 40.

77. *Id.*

78. McCormick & Gage, *supra* note 40 (discussing the qualifications of Moderators).

79. PRESIDENT’S COMM’N, *supra* note 65, at 40.

80. *See id.*

81. *See id.* at 42.

82. *See id.* at 40.

83. *See* McCormick & Gage, *supra* note 40.

84. PRESIDENT’S COMM’N, *supra* note 65, at 40.

85. *Id.* at 40-41.

86. *Id.* at 41. In order for the Associate to become a member of the family he must also be of the same ethnicity, Italian, as the family members. *Id.*

Member to become a full member, or Vendor, in a cybergang.<sup>87</sup>

The structure of a Mafia family mirrors the structure of a cybergang, but structure is not the only way that the Mafia and cybergangs are similar. The continuity and criminal nature of the Mafia is also similar to a cybergang. Just as the Mafia is designed to continue through leadership changes, so too is the cybergang.<sup>88</sup> Cybergangs and the Mafia are formed for the purpose of financial gain based on the collective knowledge of the group.<sup>89</sup> Cybergangs and the Mafia both use a wide range of tactics to continue their operations: The Mafia uses bribery, intimidation, and murder to obtain their goals, while cybergangs intimidate through the threat of computer attacks.<sup>90</sup> The structure, purpose, and continuity of the Mafia are similar to cybergangs, and these similarities may help prosecutors who are seeking more severe penalties for those participating in a cybergang.

#### D. Cybergang Tactics

Shadowcrew was not the only cybergang in existence. Shadowcrew members who avoided prosecution are alleged to be associated with other developing cybergangs.<sup>91</sup> In 2004, "Muzzfuzz" was shut down by law enforcement officers.<sup>92</sup> Muzzfuzz ran the same credit card and identification documents schemes as Shadowcrew.<sup>93</sup> "Stealthdivision," another cybergang that was shut down in 2004, was composed mainly of Shadowcrew members who eluded police when the main members of Shadowcrew were arrested.<sup>94</sup> Stealthdivision eluded capture for some time as they tricked police and investigators into believing they were operating from another country.<sup>95</sup> Stealthdivision used computers and servers located in Malaysia in order to keep investigators clueless as to their whereabouts.<sup>96</sup> In the time between both Shadowcrew's and Stealthdivision's shutdowns, Stealthdivision was able to amass

---

87. McCormick & Gage, *supra* note 40 (stating that a General Member must be vouched for to the Administrator in order to become a full-fledged member of a cybergang).

88. Compare PRESIDENT'S COMM'N, *supra* note 65, at 25 (stating that Mafia families are designed to continue over time and through changes in leadership), with McCormick & Gage, *supra* note 39 (stating how it is believed that members of Shadowcrew who avoided prosecution were linked to the formation of new cybergangs).

89. PRESIDENT'S COMM'N, *supra* note 65, at 25.

90. *Id.* at 25; see McCormick & Gage, *supra* note 40.

91. McCormick & Gage, *supra* note 40.

92. *Id.*

93. *Id.*

94. *Id.*

95. *See id.*

96. *Id.*

approximately 320 members.<sup>97</sup> “Boatfactory” and “Darkprofits” were also recently shut down for operating criminal organizations similar to Shadowcrew.<sup>98</sup>

However, all of these current cybergangs pale in comparison to the Russian cybergang, “HangUp Team,” which has eluded capture for over two years.<sup>99</sup> It is becoming clear that once cybergangs are prosecuted, the members who evaded police do not stop their criminal activities, but form new cybergangs.<sup>100</sup> FBI agent Daniel Larkin stated, “If you don’t try to take these guys down, they’ll come back. You have to find a way to get to the live bodies and take them out at their roots. If you don’t, you aren’t solving the problem.”<sup>101</sup> The reformation of cybergangs shows that they are not being prosecuted aggressively enough to prevent other gangs from forming, especially when considering the motivation behind a cybergang.

Cybergangs’ primary motivation, as stated previously, is monetary gain. In order to accomplish this goal, the gangs employ a wide range of tactics. One of the largest tools in the arsenal of a cybergang is the creation of “zombie” computers.<sup>102</sup> Zombie computers are computers that are deliberately infected with a virus that allows the creator of the virus to control certain functions of the computer despite what the actual owner of the computer is doing.<sup>103</sup> Cybergangs create “armies” of zombie PCs directly under their control which can then lead to large scale attacks on

---

97. *Id.* Stealthdivision specialized in the trafficking of stolen credit card numbers, identification documents, and contained an estimated 320 known members. Stealthdivision was a direct effort by Shadowcrew members to regroup after their demise. *Id.*

98. *Id.* Boatfactory was responsible for \$2.5 million in credit card losses. *Id.* Darkprofits was responsible for the creation of various worms which may have been used as a tool for future extortion and denial of service attacks. *Id.*

99. Grow & Busch, *supra* note 2. HangUp Team has blatantly hidden in plain sight as they have frequently left clues and digital signals claiming responsibility for numerous viruses and worms that wreaked havoc on different companies globally. *Id.*

100. TECHWEB TECHNOLOGY NEWS, *Hacker Turf War Will Lead to Large E-crime Gangs*, Mar. 18, 2005, <http://www.techweb.com/wire/security/159902363>, available at 2005 WLNR 4262631. There were early indications that the smaller cybergangs would fight over territory in cyberspace and the larger gangs would absorb the members of other gangs who have avoided detection. This would result in several very large and organized cybergangs. *Id.*

101. Grow & Busch, *supra* note 2. Daniel Larkin is the former head of the FBI’s Internet Crime and Complaint Center. *Id.*

102. See MCAFEE, *supra* note 23, at 13. Zombie PCs are computers running programs that give control to another user over the Internet. *Id.* The criminal user is able to directly command use of these computers. *Id.* When cyber criminals gain control of the infected computers they are able to execute denial of service attacks and even hide fraud behind these zombie PCs. *Id.*

103. *Id.*

targeted businesses when they are commanded to perform a malicious function.<sup>104</sup> Cybergangs are effective in utilizing this crime as they have more Associates who can infect more computers, leading to larger armies of zombie PCs.<sup>105</sup> The cybergangs take the zombie PCs and threaten to launch an attack against a company's website unless they are paid a ransom.<sup>106</sup> On one website (subsequently shut down by the government) the asking price for the temporary use of an army of 20,000 zombie PCs ranged from \$2000 to \$3000.<sup>107</sup>

The use of zombie PCs is just one way to extort money from a company; in many instances the cybergang will threaten companies or private individuals with an attack if they are not paid a large sum of money.<sup>108</sup> Hackers and cybergangs are not afraid to demand between \$20,000 and \$30,000 from corporations, threatening that if they are not paid the company will undergo a severe cyberattack.<sup>109</sup> Further, corporations will often not report the extortion for fear that this information will lower company value in the eyes of stockholders.<sup>110</sup> A company may also fear that admitting to the public that their security was breached will cause consumers to believe that the company is vulnerable to cyberattacks.<sup>111</sup> Congress recognized the growing problem of cybercrime and realized the need for computer-specific crime legislation.

### III. COMPUTER FRAUD AND ABUSE ACT

The Computer Fraud and Abuse Act (CFAA) was originally passed in 1984 in response to the growing concern over cybercrime, but was criticized as vague and too narrow in scope.<sup>112</sup> In response to concerns with the 1984 Act, Congress revised the CFAA in 1986.<sup>113</sup> The 1986 version of the CFAA created a difference between computer trespass, which was not criminal in purpose, and more damaging computer crimes.<sup>114</sup> The 1986

---

104. *Id.*

105. Spring, *supra* note 1.

106. *Id.* When a cybergang controls zombie PCs, it forces all the infected PCs to visit a website where, due to the mass influx of website traffic, the overwhelmed server shuts down the computer. This causes a loss to the business and leaves it vulnerable to further attacks. *Id.*

107. *Id.* The former website, <http://www.SpecialHam.com>, listed the price for zombie PCs along with prices for email addresses and other viruses.

108. *Id.*

109. *Id.*

110. *Id.*

111. *Id.*

112. Skibell, *supra* note 19, at 912.

113. *Id.*; see Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000 & Supp. 2003).

114. *Id.*

amendments also classified computer fraud, trafficking network passwords, and hacking as felonies.<sup>115</sup> The amendments also added an “intent” element to the hacking provision so that computer users who mistakenly caused damage or accidentally accessed information would not be prosecuted as computer criminals.<sup>116</sup> The CFAA was amended again in 1988, 1989, and 1990, but these amendments were relatively minor and only clarified existing terms.<sup>117</sup>

In 1994, the CFAA was again amended to create two more felonies.<sup>118</sup> The new amendments also departed from past Acts in that they made intentional computer trespass that results in damage a misdemeanor.<sup>119</sup> Computer crime continued to rise despite the existence of the CFAA, and Congress responded again in 1996.<sup>120</sup> The Act was broadly expanded to encompass a larger variety of crimes punishable under the Act.<sup>121</sup> Congress also changed the loss requirement from \$1000 to \$5000.<sup>122</sup>

Finally, the CFAA was again amended following the passage of the USA PATRIOT Act.<sup>123</sup> The amendments to the CFAA in the wake of the USA PATRIOT Act made significant improvements to the Act.<sup>124</sup> The new amendments mandated that the \$5000 threshold did not apply to crimes against computers that were used for national security or for criminal justice.<sup>125</sup> Congress also changed the way monetary loss would be calculated, making it easier to reach the \$5000 threshold.<sup>126</sup> The final and most important change to the CFAA was the penalty structure for crimes with complex divisions of crimes receiving punishment.<sup>127</sup>

---

115. *Id.* at 913.

116. *Id.* at 913-14.

117. *Id.* at 914.

118. *Id.* (consisting of intentional damage to a computer by knowingly transmitting a harmful program and intentional access of a computer without authorization that recklessly causes damage).

119. *Id.* The 1994 amendments, for the first time, made reckless conduct a punishable misdemeanor. *See id.*

120. *Id.*

121. *Id.* at 915.

122. *See id.* at 916.

123. *Id.* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

124. Skibell, *supra* note 19, at 916.

125. *Id.*

126. *Id.* at 916-17.

127. *See id.* at 917.

## A. Current Form of the CFAA

The CFAA classifies and punishes different computer crimes and criminalizes seven acts with respect to computers.<sup>128</sup> The first crime under the CFAA is the unauthorized access of a computer in order to gain information that foreign nations or individuals could use to injure the United States.<sup>129</sup> This provision criminalizes computer espionage.<sup>130</sup> The next provision under the CFAA is the unauthorized access provision.<sup>131</sup> Section 1030(a)(2)(A) prohibits obtaining information contained in financial records, or information used by financial companies and credit agencies.<sup>132</sup> Section 1030(a)(2)(B) criminalizes the possession of information gained through unauthorized access of a government agency's computer.<sup>133</sup>

The third provision in the CFAA governs the unauthorized access to any nonpublic computer that is used by a department or agency of the federal government.<sup>134</sup> This provision prohibits anyone from gaining access to a computer that is used exclusively by the federal government.<sup>135</sup> The fourth criminal act governed by the CFAA is computer fraud.<sup>136</sup> Section 1030(a)(4) prohibits knowingly, and with intent to defraud, accessing a protected computer without authorization and furthering an intended fraud.<sup>137</sup>

The fifth provision, section 1030(a)(5)(A), governs the damage of computers,<sup>138</sup> which prohibits anyone from knowingly transmitting code, information, programs, or commands to intentionally cause damage.<sup>139</sup> This provision is intended to punish the use of a virus, worm, or other malevolent program that damages a computer.<sup>140</sup> The sixth provision, section 1030(a)(6), forbids password trafficking,<sup>141</sup> which prohibits anyone from knowingly and intentionally trafficking passwords or other

---

128. Patrick Corbett, *State and Federal Criminal Cyberlaw and Legislation Survey*, 18 T.M. COOLEY L. REV. 7, 11-12 (2001).

129. 18 U.S.C. § 1030(a)(1) (2000).

130. Corbett, *supra* note 128, at 11.

131. 18 U.S.C. § 1030(a)(2).

132. *Id.* § 1030(a)(2)(A).

133. *Id.* § 1030(a)(2)(B).

134. *Id.* § 1030(a)(3).

135. *Id.*

136. Corbett, *supra* note 128, at 11.

137. 18 U.S.C. § 1030(a)(4).

138. Corbett, *supra* note 128, at 11-12.

139. 18 U.S.C. § 1030(a)(5)(A)(i)-(iii) (2000 & Supp. 2003).

140. Corbett, *supra* note 128, at 9.

141. *Id.* at 12.

information used to gain access to computers used by the federal government or affecting interstate commerce.<sup>142</sup> The final criminal act under the CFAA is extortion.<sup>143</sup> An individual is prohibited from attempting to extort money from any person by threatening damage to a protected computer.<sup>144</sup>

One of the main criticisms of the prior versions of the CFAA was ambiguity, especially with loss and access provisions.<sup>145</sup> Similarly, prior to the USA PATRIOT Act, courts were split on the correct way to measure loss, and whether they would be allowed to aggregate the costs of investigation or if there had to be a direct financial loss to the person or entity.<sup>146</sup> In *United States v. Middleton*, the Ninth Circuit Court of Appeals ruled that when determining loss, a court was free to look at the measures reasonably necessary to restore data and information damaged and other measures that were needed to secure the system due to the exploited breaches in security.<sup>147</sup> The *Middleton* definition was later incorporated into the CFAA with the passage of the USA PATRIOT Act.<sup>148</sup> While the expansion of this definition strengthened the CFAA by allowing the aggregate harm of computer hacks to be taken into account, the CFAA still lacks the punitive punch in sentencing that is required for cybergangs.

#### B. Penalties Under the CFAA

The penalties that are handed down through the CFAA need to be examined in order to understand why they are not effective against cybergangs. The CFAA fails to adequately address the need for strong punishments with regard to cybercrime. Just as individual criminal law did not deter the Mafia, the CFAA is not going to prevent or correctly punish existing cybergangs.

The penalties regarding cybercrime are addressed in section 1030(c) of the CFAA.<sup>149</sup> If a criminal uses unauthorized access of a computer in a manner previously discussed (violating section 1030(a)(2)), the punishment

---

142. 18 U.S.C. § 1030(a)(6).

143. *Id.* § 1030(a)(7).

144. *See id.*

145. *See* Tammy J. Schemmel, *WWW.STOPCYBERCRIME.COM: How the USA PATRIOT Act Combats Cyber-Crime*, 29 WM. MITCHELL L. REV. 921, 930-31 (2003) (stating that there was ambiguity as to how damages would be calculated).

146. Skibell, *supra* note 19, at 916-17.

147. 231 F.3d 1207, 1213 (9th Cir. 2000) (“In determining the amount of losses, you may consider what measures were reasonably necessary to restore the data, program, system, or information that you find was damaged or what measures were reasonably necessary to resecure the data, program, system, or information from further damage.”).

148. Skibell, *supra* note 19, at 917.

149. *See* 18 U.S.C. § 1030(c) (2000 & Supp. 2003).

involves a fine and imprisonment for not more than ten years if it is the first offense.<sup>150</sup> There are no cases that have been appealed or prosecuted under this provision of the CFAA as of April 15, 2007.<sup>151</sup> Similarly, the espionage section allows for imprisonment of up to twenty years for a repeat offender.<sup>152</sup> However, prosecutors are not utilizing the CFAA. Instead, in cases of espionage through use of a computer, the prosecution of perpetrators is usually done through the espionage statutes.<sup>153</sup>

The second set of punishments prescribes a fine and/or imprisonment for not more than one year if there is a violation of the unauthorized access provision, accessing nonpublic government computers, the hacking provision, or trafficking passwords.<sup>154</sup> Only if the perpetrator violates the unauthorized access provision with respect to financial institutions for private financial gain, a violation of constitutional law, or if the value of information obtained exceeds \$5000, will the possible punishment under CFAA rise to five years.<sup>155</sup>

The punishment for violating section 1030(a)(4), the computer fraud provision, is only five years imprisonment if it is the individual's first offense.<sup>156</sup> Again, the penalty is only raised to ten years if it is a repeat violation.<sup>157</sup> Similarly, if a cybercriminal tries to extort money from an individual or a company, in violation of section 1030(a)(7), the penalty is only five years imprisonment.<sup>158</sup> Cybergangs frequently use extortion through denial-of-service attacks; however, under the CFAA the maximum punishment is only five years imprisonment.

The last significant punishments under the CFAA are the penalties available for the transmission of malicious code, worms, or viruses. If an individual violates section 1030(a)(5)(A)(i), the penalty is up to ten years

---

150. *Id.* § 1030(c)(1)(A) (2000).

151. A search using Westlaw and LEXIS (Apr. 15, 2007) reveals no cases prosecuted in the federal system for a violation of 18 U.S.C. § 1030(a)(1). See Jonathan B. Wolf, *War Games Meets the Internet: Chasing 21st Century Cybercriminals with Old Laws and Little Money*, 28 AM. J. CRIM. L. 95, 110 & nn.149 & 150 (2000) (noting that at the time the article was written there were no prosecutions under 18 U.S.C. § 1030(a)(1), although violations of CFAA have likely occurred).

152. 18 U.S.C. § 1030(c)(1)(B) (2000). However, as was previously discussed, since there have been no prosecutions under section 1030(a)(1), the twenty-year imprisonment has yet to be seen.

153. Wolf, *supra* note 151, at 110.

154. 18 U.S.C. § 1030(c)(2)(A) (2000 & Supp. 2003).

155. *Id.* § 1030(c)(2)(B) (2000 & Supp. 2003).

156. *Id.* § 1030(C)(3)(A).

157. *Id.* § 1030(C)(3)(B).

158. *Id.* § 1030(C)(3)(A).

imprisonment.<sup>159</sup> The punishments that are available through the CFAA do not adequately penalize the most threatening individuals. Cybergangs' motivation is purely monetary, and, as a group of cybercriminals, cybergangs can potentially cause the most damage to computer systems. As such, cybergangs should warrant more attention and harsher penalties.

### C. Problems with the CFAA

One of the main problems with the CFAA is the overlap between cybercrime and non-cybercrime. Most of the offenses under the CFAA are recognizable non-cybercrime offenses, adapted to crimes committed with the use of a computer.<sup>160</sup> Similarly, one of the main threats of cybercrime is identity theft, especially in the form of credit card information and bank account information. However, CFAA section 1030(a)(2)(A), which addresses this concern, fails to go further than other statutes relating to bank fraud.<sup>161</sup> The CFAA fails to adequately address the problems of cybercrime because the statute only codifies prior common law crimes with respect to computers and does not address the specific techniques or crimes that cybercriminals use. For example, the Act fails to specifically address some of the main tactics that hackers use, such as denial-of-service attacks and credit card fraud.

The cybergangs that are caught and prosecuted are increasingly being charged with a multitude of offenses; however, they are not receiving the necessary punishment and attention that is needed in order for the government to take a firm stance against cybergangs. Six alleged leaders of the Shadowcrew cybergang recently pled guilty to criminal charges of credit card, bank card, and identification document fraud.<sup>162</sup> One member, Andrew Mantovani, plead guilty to one count of conspiracy and a second count of unlawfully transferring identification documents to facilitate criminal conduct.<sup>163</sup> The maximum penalty is five years imprisonment and a \$250,000 fine for each count.<sup>164</sup> Yet Shadowcrew, under the guidance of Mantovani and fellow cybergang members, was responsible for trafficking

---

159. *Id.* § 1030(C)(4)(A) (2000 & Supp. 2003).

160. Wolf, *supra* note 151, at 114 (noting that the CFAA “adds nothing to existing substantive law [but] merely replicates both the adequacies and inadequacies of existing . . . statutes.”).

161. *See id.* at 115 (noting that bank fraud statutes already cover unauthorized access to financial information and the only thing CFAA really does is address the use of a computer to gain information).

162. Press Release, U.S. Dep't of Justice, Six Defendants Plead Guilty in Internet Identity Theft and Credit Card Fraud Conspiracy (Nov. 17, 2005), <http://www.cybercrime.gov/mantovaniPlea.htm>.

163. *Id.*

164. *Id.*

an estimated 1.5 million stolen bank account numbers, amounting to over \$4 million in losses.<sup>165</sup> The members of this cybergang were not charged with any provision under the CFAA, the alleged main weapon for combating computer crime.<sup>166</sup> Would the prosecutors feel this was a victory if the head of a Mafia family, responsible for millions of dollars in stolen financial information, was charged with one count of conspiracy and faced a maximum of five years imprisonment?

Patrick Gregory, another member of famed cybergangs “total-kaOs” and “globalHell,” recently pled guilty to one count of conspiracy to commit telecommunications fraud and computer hacking.<sup>167</sup> Gregory was sentenced to twenty-six months imprisonment and fined for his part in the illegal intrusions he caused in the telecommunications industry, which were estimated to be around \$1.5 to \$2.5 million.<sup>168</sup> Further, another member of “globalHell” pled guilty and was sentenced to six months imprisonment and fined.<sup>169</sup> A member of “the Darkside Hackers” was sentenced to twenty-one months imprisonment and a \$3000 fine (plus nearly \$90,000 in restitution) after his group caused over \$90,000 in damage to an Internet Service Provider.<sup>170</sup> Again, although this individual could have been found in violation of the CFAA, he was instead charged with possession of unauthorized access devices.<sup>171</sup>

Another main problem with respect to cybergangs and the CFAA is the failure of many businesses to report illegal intrusions or extortion attempts. According to early surveys of computer crime, only thirty-two percent of computer intrusions are reported to law enforcement agencies.<sup>172</sup> Businesses often explain that their failure to report computer security breaches stems from the fear that consumers will lose confidence in their security, that competitors may try to capitalize on the company’s weakness,

---

165. *Id.*

166. *See id.* The charges against Mantovani and others associated with Shadowcrew fail to indicate that they have been charged under section 1030(a)(2)(A) or section 1030(a)(4). *Id.*

167. Press Release, U.S. Dep’t of Justice, Computer Hacker Sentenced (Sept. 6, 2000), <http://www.cybercrime.gov/gregorysen.htm>.

168. *Id.*

169. Press Release, U.S. Dep’t of Justice, Chad Davis, “Global Hell” Hacker, Sentenced to Six Months in Prison, Three Years Probation, For Air Force Network Hacks (Mar. 1, 2000), <http://www.cybercrime.gov/davis.htm>.

170. Press Release, U.S. Dep’t of Justice, Computer Hacker Sentenced in Federal Court (July 24, 2000), <http://www.cybercrime.gov/miffle2.htm>.

171. *See id.*

172. Wolf, *supra* note 151, at 102. According to a 1999 computer crime survey done by the Computer Security Institute, the numbers in reported attacks has risen, yet is still extremely low. *Id.* at 102 & n.57.

and that law enforcement is not concerned with computer crime.<sup>173</sup> This ultimately means that computer hackers, especially cybergangs that have the ability to inflict much greater harm than a single hacker, are not being deterred from their illegal activities since many businesses do not report these intrusions.<sup>174</sup> Similarly, a lack of reporting and weak laws enabled organized crime to thrive before the enactment of RICO.<sup>175</sup> Since the CFAA is not being used to prosecute cybergang members, the government should be using the same tactics they use to fight traditional organized crime. RICO needs to be utilized to make prosecution of cybergangs more effective.

#### IV. RICO: PROSECUTING CYBERGANGS

In response to the growing problem of organized crime, Congress enacted RICO as Title IX of the Organized Crime Control Act.<sup>176</sup> Congress determined the most effective strategy to combat organized crime was not to charge individual members with specific crimes, but, instead to prohibit the criminal organization.<sup>177</sup> RICO was a successful strategy that worked against organized crime due to a continued long-term enforcement campaign.<sup>178</sup> Powerful criminal and civil RICO statutes, along with continuing attention from law enforcement, caused the future of the Mafia to be questioned.<sup>179</sup> Therefore, if criminal and civil RICO statutes work against the traditional forms of organized crime, the question must be asked, will they work against cybergangs—the twenty-first century computer-based organized crime. Since the CFAA is not frequently used to prosecute computer crime, other laws are being adapted to prosecute

---

173. *Id.* at 102-03.

174. *See generally id.* at 102-05. The author notes the weakness in the CFAA and law enforcement techniques, as well as a perception that the FBI lacks sensitivity to businesses' needs. *Id.* at 103.

175. *See* Brian Goodwin, *Civil Versus Criminal RICO and the "Eradication" of La Cosa Nostra*, 28 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 279, 279 (2002) (noting that the "eradication of organized crime in the United States" was a primary reason for enacting RICO).

176. *Id.* at 293; *see* Racketeer Influenced and Corrupt Organizations Act, 18 U.S.C. §§ 1961 to 1968 (2000 & Supp. 2003).

177. *Id.* at 292.

178. *See id.*

179. James B. Jacobs & Lauryn P. Gouldin, *Cosa Nostra: The Final Chapter?*, 25 CRIME & JUST. 129, 158 (1999) (noting that due to long time government support, the RICO statutes, and the continued assaults on organized crime, the survival of the La Cosa Nostra is in jeopardy).

computer criminals. Therefore, RICO should be used to prosecute, and ultimately deter, the formation of cybergangs.

#### A. RICO Act Requirements

First, section 1962(a) makes it illegal for any person to receive any income from a pattern of racketeering activity through the running of a criminal enterprise.<sup>180</sup> The Act requires that there be: “(1) conduct (2) of an enterprise (3) through a pattern (4) of racketeering activity.”<sup>181</sup> A person, as defined by RICO, is “any individual, or entity capable of holding a legal or beneficial interest in property.”<sup>182</sup> An enterprise is defined as “any individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated in fact although not a legal entity.”<sup>183</sup> Organized crime groups are included in the classification of enterprise.<sup>184</sup> A “pattern of racketeering activity” is defined as at least two acts of racketeering activity that occurred within ten years of each other after the effective date of RICO.<sup>185</sup> Section 1961(1)(B) defines “racketeering activity” as any act which is indictable under an enumerated list of federal violations under Title 18 of the United States Code, such as extortionate credit transactions (section 1028), or bribery (section 201).<sup>186</sup>

The U.S. Supreme Court has found that because RICO is directed toward an organization, the pattern of racketeering activity must have “continuity plus relationship” between the criminal acts.<sup>187</sup> The Court also stated that in order to establish the relationship prong there must be some connection between the acts, such as similar results of the crime,

---

180. 18 U.S.C. § 1962(a) (2000).

181. *See Sedima, S.P.R.L. v. Imrex Co., Inc.*, 473 U.S. 479, 496 (1985) (footnote omitted).

182. 18 U.S.C. § 1961(3) (2000).

183. *Id.* § 1961(4).

184. Goodwin, *supra* note 175, at 298; *see United States v. Turkette*, 452 U.S. 576 (1981).

185. 18 U.S.C. § 1961(5) (2000).

186. *Id.* § 1961(1)(B) (2000 & Supp. 2003). “Racketeering activity” is defined as “any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical . . . which is chargeable under State law and punishable for more than one year.” *Id.* § 1961(1)(A) (2000 & Supp. 2003). Section 1961(1)(B) lists a host of violations that count as racketeering activity.

187. *See Sedima, S.P.R.L. v. Imrex Co., Inc.*, 473 U.S. 479, 496 & n.14 (1985) (italics omitted) (legislative history and Senate Reports make clear that the threat of continuing racketeering activity is necessary under RICO); *see also* Goodwin, *supra* note 175, at 293.

participants, victims, or purposes.<sup>188</sup>

The criminal sanctions in RICO are severe and are designed to eradicate organized crime.<sup>189</sup> Section 1963(a) directs that anyone found violating section 1962 shall be fined or imprisoned for not more than twenty years.<sup>190</sup> The section also states that certain violations based on racketeering activity carry a maximum sentence of life imprisonment.<sup>191</sup> The criminal sanctions also mandate that any interest in property or business obtained through the racketeering activity acquired in violation of section 1962 shall be forfeited.<sup>192</sup> Recommendations to ignore the Federal Sentencing Guidelines are frequently made.<sup>193</sup> Often the courts may ignore sentencing guidelines due to the heinousness of the offense or due to the possibility of continued criminal activity.<sup>194</sup> The sentences mandated under RICO aim to eradicate the Mafia and organized crime; severe penalties accomplish these established goals.

#### B. RICO Applied to Cybergangs

The CFAA, as previously stated, is not being used frequently for prosecuting computer crime.<sup>195</sup> Since cybergangs pose far more danger than the average computer hacker and are similar in structure to organized crime, they need to be treated as organized crime and punished by RICO provisions. Evidence acquired from the Shadowcrew prosecutions shows that cybergangs can be prosecuted under RICO. RICO requires that a person receive income from certain prohibited activities.<sup>196</sup> The definition also points out that a “person” is anyone who is capable of holding a legal or beneficial interest in property.<sup>197</sup> Mantovani, the alleged ringleader of the Shadowcrew gang, received a share of the income that other members made through their illegal activities.<sup>198</sup>

Shadowcrew and other cybergangs are “enterprises,” the next factor required by RICO. Shadowcrew and other cybergangs are comprised of a group of individuals associated-in-fact, even though they are not

- 
188. *Sedima*, 473 U.S. at 496 n.14.  
189. Goodwin, *supra* note 175, at 299-300.  
190. 18 U.S.C. § 1963(a) (2000).  
191. *Id.*  
192. *Id.*  
193. Goodwin, *supra* note 175, at 300.  
194. *Id.* at 292.  
195. *See infra* Part III.B.  
196. 18 U.S.C. § 1962(a) (2000).  
197. *Id.* § 1961(3) (2000).  
198. McCormick & Gage, *supra* note 40.

considered a legal entity.<sup>199</sup> If traditional organized crime falls within the definition of an enterprise, then similarly there should be no distinction of organized crime perpetrated through the Internet or by computer.<sup>200</sup> Further, Shadowcrew was a continuous organization, operating well past their first credit card scheme, with no known intention to limit their crimes to one credit card theft or fraudulent transaction.<sup>201</sup> Shadowcrew members shared a common purpose, looking to capitalize on each other's computer hacking knowledge in order to maximize their profits. Shadowcrew was clearly an organized group or association—in structure a virtual Mafia family. Just as Mafia families are found to be enterprises, so too should cybergangs.<sup>202</sup> Common purpose or common criminal scheme is also a prominent factor in finding an enterprise.<sup>203</sup> Shadowcrew was formed for the common purpose of committing identity theft and credit card fraud in order to make a profit.<sup>204</sup> Therefore, cybergangs qualify as enterprises.

The next factor to establish a RICO charge is the pattern requirement.<sup>205</sup> The Supreme Court stated that in order to show a pattern of activity, there must be continuity and relationship.<sup>206</sup> In order to prove continuity and relationship, the prosecution must show that the acts are related and amount to a threat of continued criminal activity.<sup>207</sup> In order to prove “relationship,” the acts or pattern of acts must somehow connect to one another by showing one of the following: similar purposes, results, participants, victims, or methods of committing the crimes.<sup>208</sup>

In the case of cybergangs there is a pattern of racketeering activity and a

---

199. See *id.* § 1961(4).

200. See generally *United States v. Turkette*, 452 U.S. 576 (1981).

201. See Goodwin, *supra* note 175, at 298 (citing *United States v. Perholtz*, 842 F.2d 343, 362 (D.C. Cir. 1988) (for the factors required to prove an enterprise: “continuity, unity, shared purpose and identifiable structure”). The government investigated Shadowcrew for more than a year, proving they had a continuous operation that may not have ceased had investigators not found them. McCormick & Gage, *supra* note 40.

202. Goodwin, *supra* note 175, at 298-99 (noting that groups, crews, commissions of mob leaders, organized crime families, and the entire La Cosa Nostra syndicate have been found to be “associated in fact” under RICO).

203. See Goodwin, *supra* note 175, at 299.

204. McCormick & Gage, *supra* note 40.

205. 18 U.S.C. § 1962(a) (2000) (“It shall be unlawful for any person who has received income derived, directly or indirectly, from a *pattern* of racketeering activity . . . to use or invest . . . [in] any enterprise which is engaged in . . . interstate or foreign commerce.”) (emphasis added).

206. *Sedima, S.P.R.L. v. Imrex Co., Inc.*, 473 U.S. 479, 496 n.14 (1985); see Goodwin, *supra* note 175, at 296-97.

207. Goodwin, *supra* note 175, at 296-97 (citing *H.J., Inc. v. Nw. Bell Tel. Co.*, 492 U.S. 229, 239 (1989)).

208. *Id.* at 297 (citing *H.J., Inc.*, 492 U.S. at 239-43; *Sedima*, 473 U.S. at 496 n.14).

continuity and relationship in their crimes. The criminal acts of Shadowcrew and other cybergangs are related to each other and to the enterprise they represented. In Shadowcrew's case, the credit card theft helped the gang gain notoriety, enabling them to grow and commit more criminal acts with their increased membership and wealth.<sup>209</sup> Their credit card theft had continuity because the acts occurred in similar ways, such as with the use of viruses, computer worms, and other forms of computer hacking.<sup>210</sup> Had the cybergang not been stopped, the credit card and identity theft would have continued and, therefore, would have remained a continuing threat of criminal activity.<sup>211</sup>

Cybergangs, like the Mafia, are seen as a continuing threat of criminal activity in their formation and tactics.<sup>212</sup> Just as section 1961(5) requires, Shadowcrew was responsible for more than two predicate acts by stealing over 1.5 million credit card numbers and more than \$4 million.<sup>213</sup> The criminal acts that cybergangs have been charged with could have been filed as predicate acts under RICO according to a list in section 1961(1)(B),<sup>214</sup> which includes acts in violation of 18 U.S.C. § 1028 for "fraud and related activity in connection with identification documents,"<sup>215</sup> 18 U.S.C. § 1029 for "fraud and related activity in connection with access devices,"<sup>216</sup> 18 U.S.C. § 1344,<sup>217</sup> and 18 U.S.C. § 1951, which could be used when cybergangs use threats of computer attacks to extort money from

---

209. See McCormick & Gage, *supra* note 40.

210. See Grow & Busch, *supra* note 2.

211. Goodwin, *supra* note 175, at 296-97 (citing *H.J., Inc.*, 492 U.S. at 239-43; *Sedima*, 473 U.S. at 496 n.14).

212. Grow & Busch, *supra* note 2 (citing an FBI agent involved in the capture of Shadowcrew that stated that cybergangs must be stopped now or they will continue to form).

213. 18 U.S.C. § 1961(5) (2000) ("pattern of racketeering activity requires at least two acts of racketeering activity").

214. *Id.* § 1961(1)(B) (2000 & Supp. 2003) (listing crimes chargeable as racketeering activity).

215. *Id.* (citing 18 U.S.C. § 1028(a)(2) (2000 & Supp. 2003) ("knowingly transfers an identification document, authentication feature, or a false identification document knowing that such document or feature was stolen or produced without lawful authority").

216. *Id.* (citing 18 U.S.C. § 1029 (2000 & Supp. 2003)). This is often the crime with which hackers are charged. See Press Release, U.S. Dep't of Justice, Computer Hacker Sentenced in Federal Court, (July 24, 2000), <http://www.cybercrime.gov/miffle2.htm> (stating that computer hacker involved in cybergang was charged with violation of 18 U.S.C. § 1029 fraud in connection with an access device).

217. 18 U.S.C. § 1061(1)(B) (citing 18 U.S.C. § 1344 (2000)) (the bank fraud provision). See McCormick & Gage, *supra* note 40 (stating again that Shadowcrew was responsible for millions in losses to banks and lending institutions).

companies.<sup>218</sup> Cybergangs, as evidenced by the damage Shadowcrew inflicted on the public, fall within the pattern of racketeering activity with at least two predicate acts.

Therefore, cybergangs do avail themselves to the threat of prosecution under RICO statutes. Cybergangs contain members who seek to profit from their activities in the gang. The gangs are enterprises due to their criminal structure and association-in-fact. The cybergangs also engage in a pattern of activity that is continuous in nature, and acts related to both the criminal enterprise and each other. Lastly, the criminal activities for which cybergangs are notorious are all covered under the definition of racketeering activity.<sup>219</sup> Therefore, cybergangs lend themselves to prosecution under the federal RICO statute.

#### V. CONCLUSION

Cybergangs are *not* comprised of harmless hackers seeking knowledge; they are criminals who, like the Mafia, seek monetary gain.<sup>220</sup> Cybergangs form and grow for the purpose of increasing the profits beyond that which an individual hacker could make.<sup>221</sup> Due to the criminal purpose of cybergangs, they need to receive closer attention than the current law affords. Just as the Mafia became an increasingly problematic source of crime during the 1970s and 1980s, cybergangs are the new form of the Mafia in the twenty-first century.

Regular criminal prosecutions before RICO did not deter the Mafia, such as prosecutions for basic assault, but when the civil and criminal RICO provisions were applied the Mafia began to fall.<sup>222</sup> Similarly, cybergangs are not going to be deterred by regular prosecutions under the CFAA or varying state laws. Because the CFAA fails to address the actual nature of computer crime, but instead merely reenacts previous criminal law with respect to computers,<sup>223</sup> cybergangs are not being prosecuted to the extent necessary to deter and punish their acts.

The CFAA fails to adequately punish members of cybergangs, and, therefore, prosecutors should revert to using RICO statutes in a similar fashion to the way they were used to combat the problem of traditional

---

218. 18 U.S.C. § 1951(a) (2000) (“Whoever in any way or degree obstructs, delays, or affects commerce or the movement of any article or commodity in commerce, by robbery, or extortion . . .”).

219. *See* 18 U.S.C. § 1961(1)(B).

220. Spring, *supra* note 1.

221. *See id.*

222. *See* Goodwin, *supra* note 175, at 280.

223. *See* Wolf, *supra* note 151, at 115.

2007]

*PROSECUTING CYBERGANGS*

575

organized crime. Many of the cybergangs' activities lend themselves to prosecution under RICO. Using RICO statutes to prosecute cybergangs would allow prosecutors more efficient methods of evidence gathering, more severe penalties, and the ability to once and for all stop cybergangs before they grow into the problems reminiscent of Mafia endeavors. Until the CFAA is amended to include specific computer crimes that cybergangs commit, RICO statutes should be used to prosecute cybergang members.

*Scott Zambo*

576

*CRIMINAL AND CIVIL CONFINEMENT*

[Vol. 33:551