A multiyear collaboration between a UK technology crime detective and the Russian MVD, while successful in the arrest, conviction and imprisonment of three hackers, also provides some of the strongest evidence to date that the Russian government is protecting some of the worst cyber-criminals on the planet.

A longtime British detective, whose name will be revealed at Black Hat, was deployed by the UK National Hi-Tech Crime Unit to Russia after a hacking ring began a series of denial-of-service attacks on legal gambling sites operating out of England, seeking extortion payments in the tens of thousands of dollars.

He spent the better part of three years working in Russia, embedding with the Russian Interior Ministry, or MVD, in what was likely the closest cooperation with Western law enforcement there in more than a decade. The team traced the Internet Protocol addresses of individuals including Ivan Maksakov, Denis Stepanov and Alexander Petrov and seized hard drives from the first two: Petrov's computer disappeared after his father, a police chief in the large city of Astrakhan, learned of the investigation.

Maksakov cooperated extensively, telling the MVD and the NHTCU detective that he worked for the other two and for men higher up in an extensive underground hierarchy that performed careful research on prospective targets, using "bots" to mask reconnaissance clicks and messaging employees to glean as much as possible about the network architecture.

Maksakov earned $1,000 or less per successful attack, with larger cuts going to a chain of middlemen. At the top were those who advertised on CarderPlanet and other bazaars of the cyber underground. All three of those arrested in 2004 and 2005 were convicted in 2006 after a closed trial in Balakovo and sentenced to 8 years hard labor.

But when the British detective tried to go after higher-ranking members of the cyber mafia, he ran into a series of obstacles, as detailed in the presenter's book "FATAL SYSTEM ERROR: The Hunt for the New Crime Lords Who Are Bringing Down the Internet" (PublicAffairs: Jan. 26, 2010). A trio strongly suspected of being involved in hiring Maksakov's gang, including one member with the honorific title of Gabelotto on CarderPlanet, wasn't prosecuted after local police said they found insufficient evidence.

A raid in St Petersburg on a hosting company used by another powerful ally, known as Bra1n, went awry after that company was apparently tipped off by corrupt officials there. The British detective and the MVD used a circular saw to get through a bank vault door guarding the machines, only to find a dumbwaiter that had been used to spirit the servers away, leaving one cable still swinging.

Worst of all were the barriers to apprehending a man known as King Arthur. The associate of Stepanov once ran the seminal crime site CarderPlanet and was famed for his ability to encode bankcards that could be used to withdraw cash from ATMs. King Arthur was suspected of directed the "cashing" that brought in millions, along with the underlying phishing campaigns against customers of Citibank and other institutions that netted the needed account numbers.

He was believed to have supervised a Texas criminal named Doug Havard, who had been picked up by the NHTCU in England, and Stepanov said he was so powerful that he was afraid that he would be killed if the two ever had a falling-out. After dogged work by US Postal Inspector Greg Crabb, lawmen had a real name to go with King Arthur's moniker, also to be revealed at Black Hat.

But when the UK detective pressed his friends at the MVD to go after King Arthur, he was first told that the man "was a nobody" making $200 a month. Then he was told that King Arthur lived in a near-lawless region. Finally, the truth came out: the FSB, the successor to the KGB spy agency that is the most powerful force in Russia, knew about King Arthur and wasn't interested in arresting him.

According to law enforcement in the US and UK, this is not due to garden variety corruption but because King Arthur has the skills and connections to assist Russia in massive denial-of-service attacks against international and domestic opponents of the FSB.

This conclusion fits with independent analysis by security researchers such as Joe Stewart, Don Jackson, Jart Armin, and Kim Zenz, as explained in Fatal System Error.

Yet even as the pattern is repeated, most recently with the Heartland Payment Systems indictment of top US identity thief Albert "Segvec" Gonzalez' unnamed Russian mentors, "Hacker 1" and "Hacker 2," government officials have said nothing critical of the Russian government. On the contrary, as they have for years, when US law enforcement agencies agree to talk at all on the subject, they say cooperation is good and getting better, and the proof is right around the corner.

Given how rapidly the cyber-security situation is deteriorating and how poorly Western financial institutions are equipped to deal with the ongoing surge in online robbery, the public deserves an honest explanation of what is happening, why, and what is being done.