Top Secrets

A world-class second on operational security at world championship matches

BY **GM PETER HEINE NIELSEN**

THE STAKES DON'T GET HIGHER in chess than the world championship, and the contenders pick assistants they can trust. In the digital age, that means more than just finding someone who won't blab your opening prep to the other team at the bar. A team needs to keep their preparations, their conversations, sometimes even their roster, secret for as long as they can, and if they're working together remotely, there's a whole invisible layer of threats to their communications.

GM Peter Heine Nielsen knows what it takes: He acted as a second on the winning side of seven straight world championship matches, working for Viswanathan Anand from 2006 to 2012 and for Magnus Carlsen since 2013. He recently shared with Chess Life *some of his experiences, and reflected on how the challenges have changed in the battles for the crown.*

My introduction to basic operational security came at the 2007 World Championship Tournament in Mexico, where I was GM Viswanathan Anand's second. He told me to at least lock my computer when leaving my hotel room, so anyone trying to access my computer would have to enter the Windows password. After I got back from Mexico, with Vishy being the new world champion, and me having lots of free time with no urgent opening work to do, I decided to see how quickly I could get access to my own computer without using the password.

All it took was a simple Google search. I downloaded a Linux disk image, burned it onto a DVD, and booted my computer with the DVD in the drive. Soon I could see and change the password, and I had access to the file structure. Start to finish, it took me less than an hour.

The intruder

By the 2010 world championship match in Sofia, things had changed. I was headed out for dinner with the other seconds one night and realized I had forgotten something in our work room. When I went back to get it, I was surprised to find all the lights had been turned off, and someone was walking around the room with a small flashlight.

To my surprise, and relief, it was one of our team members. I had been told he was there to help with "practical matters," but as it turned out, he was responsible for security. Anand was defending his title against GM Veselin Topalov on the challenger's home ground in Bulgaria, and our guy was checking the work room for bugging devices. (He told us he used to work for either the CIA or FBI, as I recall, and he did have a jacket with their name on it, although I assume that can be bought in any souvenir shop, and it is entirely possible he was just joking.)

I am not really of the suspicious type, so the possibility that we'd been bugged hadn't crossed my mind. But after Game 2 I had a short conversation with fellow second GM Rustam Kasimdzhanov, where we discussed the fact that our opponent had hit exactly at two very weak spots in our preparation. Did they actually have access to our pre-match notes? It was a time when several people had

IMAGE: FREEPIK

voiced some suspicions against Topalov. To be fair, Vishy won that match, and losing is a convincing way to clear yourself from having cheated, at least in that specific match.

By 2016, I had started to work for world champion Magnus Carlsen. He defended his title that year in New York against GM Sergey Karjakin, whose stated ambition was "to bring the title back to Russia." The world was still learning about the extent to which Russia had cheated at the 2014 Sochi Winter Olympics, and the Russian state cares a lot about chess — there are very direct ties between the Kremlin and the leadership of the Chess Federation of Russia. Even though we had friendly personal relations with Karjakin's lead second, GM Vladimir Potkin, we had to consider the possibility that someone would try to access our preparation to help Karjakin, even behind the backs of the challenger and his team.

Magnus signed a sponsorship agreement with IBM, and one of their top managers, who had a past in the intelligence service, helped us set up some precautions. It included new email addresses, new laptops with extra hardening, and more.

As far as security went, it was a success — but it interfered considerably with our workflow. In a team of five seconds, we exchange files constantly, and using a secure system becomes a nuisance. The IBM sponsorship included access to cloud computing power, but that required logging on and off whenever you wanted to use an engine. That might only take a minute or two each time you start Stockfish, but it becomes an issue when it intrudes on very basic routines you do several times during a day, under stressful conditions when the match is ongoing — especially when you're defending yourself against a threat you feel is most likely imaginary.

Social media self-owns

As we saw in the 2018 Carlsen – Caruana match, one's own content production can pose a bigger security risk than foul play by the opponent. During the match, Team Caruana published a promotional video during the match from a training camp, and one short clip portrayed lines of opening research in the Petroff, Queen's Gambit Declined, and Grünfeld Defense on a computer screen. (See photo below.) We did try to exploit that by targeting a specific line in the Petroff based on the leak, but it failed spectacularly, as we guessed their next move wrong.

It's not as well known, but we had our own incident in Team Carlsen: Before the match, the media team published a video from a training camp which included a few seconds of GM Daniil Dubov sitting on a sofa. Dubov is perhaps the world's leading expert on the Sveshnikov Sicilian, and he helped us prepare it for the match. I threw a small tantrum when the video was released, angrily stating that after working on the Sveshnikov for months, we essentially had given away any kind of surprise value. But the video was taken down after about a half-hour, and to the best of my knowledge, nobody seems to have noticed.

Other online accidents

In 2021, Magnus faced GM Ian Nepomniachtchi, another challenger with strong financial backing and a stated aim to bring the title back to Russia. Based on our experience from 2016, we were reluctant to go for a very secure solution — partly because it strained our workflow, but also because it felt naive to actually believe we could protect our files, if someone seriously wanted to access them. Dubov was again part of our team, and he lives in Moscow; all that would be needed was to physically access his laptop, or to install some kind of simple spy software.

Once again, internal, accidental leaks were the relevant issue: During one of the games it turned out that someone was leaving "footprints" in the ChessBase "Let's Check" database!

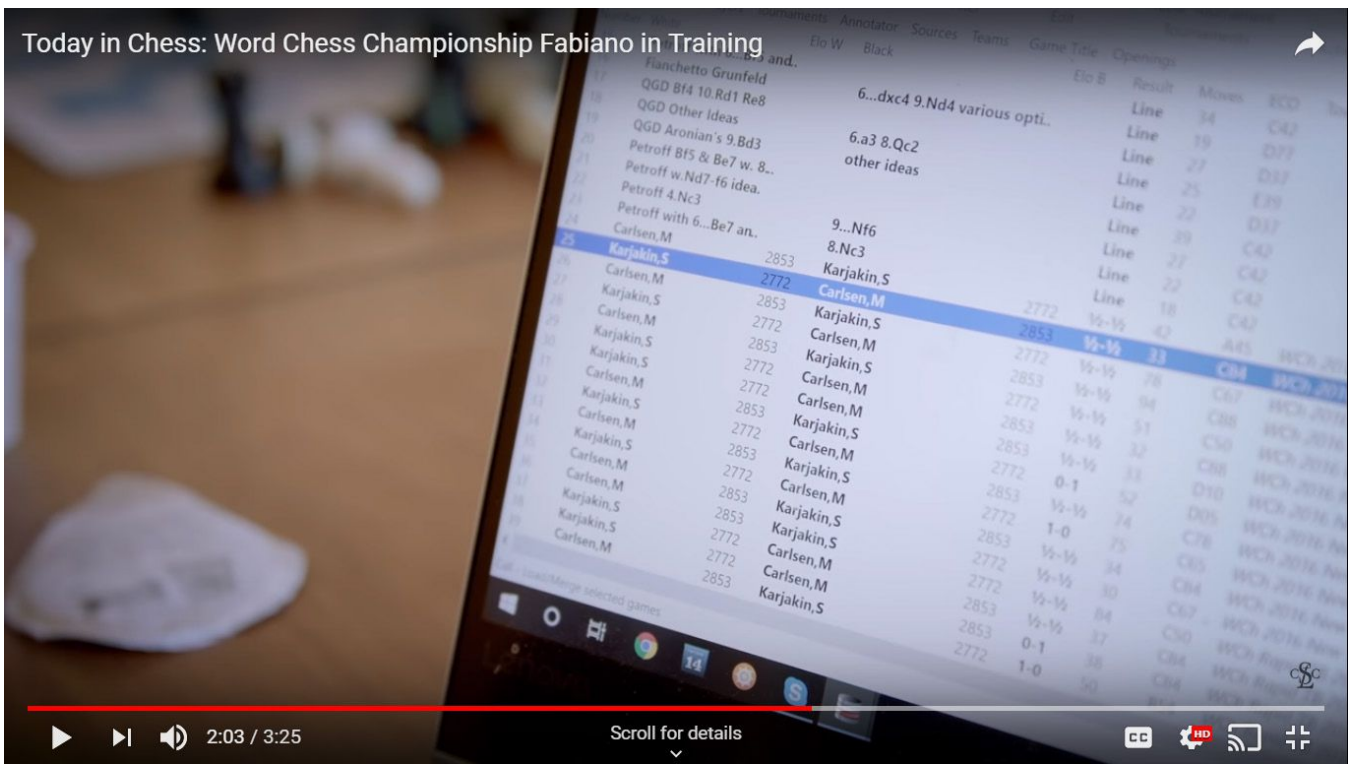

PHOTO: HARTMANN ARCHIVES

"Let's Check" is an optional ChessBase feature that allows users to contribute engine evaluations to a global database of positions. What happened was simple: Someone had forgotten to unclick the "connect automatically" setting in "Let's Check," and they left traces of their analysis in the cloud database for anyone to see. It's a fun tool if the idea is general growth of the game, but it's obviously problematic for people wanting secrecy!

(Team Ding came up with their own "improved" version of this blunder for the 2023 match, having played training games on the Lichess server using anonymous accounts. The problem was, they had forgotten to consider that once one of the ideas from the training games was used in the actual match, a simple search in the Lichess database would expose the training games in the line, and by checking the games of the account who played the idea, a number of ideas not yet implemented could be found.)

Back to 2021: As mentioned, we decided not to overthink our operational security. I knew what the top levels of security were like — my wife, GM and former European women's champion Viktorija Čmilytė-Nielsen, was speaker of the Lithuanian Parliament, and was under 24/7 protection by the state. It was obvious that the security resources for her were completely unrealistic for a chess team of five seconds living in different countries and collaborating on laptops, phones and more.

I was told to research a bit and use common sense, based on the understanding that if someone seriously tried to gain access, they would succeed anyway. I was just told to have a very basic layer of security and try to make sure there were no accidental leaks.

Just in case

Some COVID-19 restrictions were still in place at the time, so we had some backup plans — we set up a B-team, or, rather, a B-person. Our concept was that the seconds would stay in Thailand, while the match was played in Dubai, but there was a risk: If the seconds tested positive, they might be quarantined by the state, or become so sick that they could not work.

So we hired GM Grzegorz Gajewski as a backup, without the knowledge of the other seconds, and had some rudimentary opening alternatives ready in case the seconds in Thailand were quarantined. But we considered Gajewski a further insurance policy in case our team preparation was exposed. No one knew about him except for Magnus and me.

As on Team Anand, my role was to spend a lot of time coordinating tasks and files, and always making sure we had a set of up to date and "clean" notes — also difficult with five people working independently at the same time, and sometimes on the same files. It very quickly becomes a mess if not properly coordinated; files and (even worse) conclusions about various lines can get messed up.

Nielsen (center left) and Carlsen (center right) in 2016

PHOTO: LENNART OOTES

Splitting up the work

I was in effect the leader of the team, even though no such formal role existed; I was the person with access to Magnus, and it was my role to act as a bridge between him and the seconds.

The work routine was that after a game, on days when another game was scheduled the next day, I would have a short conversation with Magnus about his intentions for the next game, during which I might pitch a few recommendations from the seconds. Then I would go to my room and call the seconds in Thailand to brief them on Magnus' wishes, debate which direction we should take, and delegate the work.

Thailand is three hours ahead of Dubai, so while it was night at the playing venue, and Magnus (and even I!) could get some sleep, the seconds could keep working during the day at their location. I would then wake up in the morning and get in touch with the other seconds, who would brief me on where things were. Unless there was some severe crisis, I would go and have breakfast before returning for the final stretch until the agreed deadline, when Magnus had to be emailed the files containing our joint work.

Our basic security level included new, dedicated email addresses on the encrypted Proton Mail server from Switzerland. But of course, during the last hours before the deadline, email discussions were too slow. We used a group chat to make sure all the details were correct. Sometimes it was methodical; sometimes, it was chaotic. But in many ways they were some of my most memorable work experiences, with everybody being completely in the zone, obviously scared to make mistakes, working together to get the files ready and to the point.

Part of the problem is that Magnus had a limited amount of time to look at the material before each game, and we had to strike a balance between making sure the information was complete enough while also limited and understandable. Seconds will sometimes get into a fight over this; they're protective of their ideas, or perhaps they want to overexplain them, fearing getting the responsibility if something goes wrong

in their line. Some will send a new idea well after I said the files were "closed," and we needed to focus on rechecking.

You are NOT invited to the chat

What is written in such a chat, a few hours before a world championship game, obviously is extremely sensitive — we discuss the sore spots of our preparation, what we must fear, and what parts of our concept are pure bluff. Having access to our pre-match notes of course would be a blow, but having access to our group chat in real time could be match-deciding.

But I am proud to state that we were well ahead of our time — we used the encrypted Signal app that's been in the news so much recently. And we managed to avoid adding any chess journalists to the chat!

OPSEC FOR AMATEURS

by John Hartmann

MOST PEOPLE DON'T NEED TO WORRY ABOUT SPIES STEALING THEIR opening files, but everyone could tighten up their online security a bit.

You already know the basics: Don't share passwords with others, and try not to repeat them on too many websites. Be sure that the links you click actually take you where you're trying to go — one popular scam involves redirecting URLs to websites that look like your bank or PayPal, but are really fakes.

Sometimes people aren't who they appear to be online. If "Vladimir Kramnik" messages you out of the blue and asks you, his "biggest fan," to send money to fund his anti-cheating initiatives, I assure you it's not really him. The real "police" will not ask you to buy an Apple gift card to settle an outstanding warrant, and you can't fix a "jury duty summons" with them either. Anytime anyone you don't know asks you to buy/send gift cards, it's a giant red flag.

Chess players should take the same general precautions in protecting their chess data as they would with other important files. Regular backups are a must, both in the cloud and in an off-site location. One idea is to copy critical data to a flash drive every month and stash it in your desk at work, just in case disaster strikes your home.

ChessBase users should take special care when working with files that are stored in the cloud. If your opening analysis lives on Dropbox or OneDrive, you should pause those services while you are writing to the files or saving new data. Otherwise your files could become corrupted when you write to them.