

TechTarget and Informa Tech's Digital Businesses Combine.

**ComputerWeekly.com**

Home &gt; Regulatory compliance and standard requirements

DONFIORE - FOTOLIA



## NEWS

## Russia hacked ex-MI6 chief's emails – what they reveal is more Dad's Army than deep state

A Russian hacking group that published emails of ex-MI6 chief Richard Dearlove claimed to have uncovered a conspiracy, but it was more Dad's Army than the 'deep state', Computer Weekly and Byline Times reveal

By **Sophie Hill**

Published: 15 Jan 2024 15:18

Reporting by: **Bill Goodwin, Duncan Campbell, Crina Boros**IT support: **Matthew Fowler**. Interactive graphics: **Sophie Hill**

A Russian hacking operation claimed to have uncovered a conspiracy among the pro-Brexit British establishment, but the paranoia-fuelled septuagenarians the hackers targeted are more Dad's Army than the "deep state".

Leaked private emails reveal how a former head of MI6 and an eccentric

historian planned a political influence campaign that reached MPs, government ministers and Number 10. Together, Richard Dearlove and Gwythian Prins mobilised a network of right-wing elites, including a Marquess, a major general and a publishing tycoon.

Fuelled by paranoia about the “Soros-funded remainiac operation”, the “Green blob”, and the Chinese Communist Party, these establishment septuagenarians were ready to defend the nation using every weapon in their arsenal – from op-eds to “black ops”.

Their elaborate schemes included hiring ex-MI6 operatives to spy on “remainers”, running a “mole” in the civil service, providing secret briefings to prime minister Boris Johnson on the dangers of Chinese telecoms company Huawei, and trying to convince the government to put the editors of a leading science journal under state surveillance.

### **‘Sneaky strawhead’**

In April 2022, a cache of over 22,000 emails from a network of encrypted Protonmail accounts belonging to pro-Brexit members of the British establishment were published online, at a URL containing the phrase “[sneakystrawhead](#)”. Security experts believe the Russian-linked hacking group Star Blizzard (also known as Coldriver, Seaborgium and Callisto) was behind the leak.

The site was registered days after the UK prime minister went on a televised walkabout with President Volodymyr Zelensky, a move that provoked fury from the Kremlin. The site presented the emails as evidence that “sneaky strawhead” (apparently a nickname for Johnson, referring to his unkempt hair) was a “puppet” of “coup plotters”.

---



But the site failed to get much attention. The first media coverage appeared several weeks later on the pro-Kremlin American news site The Grayzone. The UK government has [warned](#) that these leaks are part of “Russia’s sustained attempts at political interference” and that the hacking group Star Blizzard is run by Russian intelligence officers.

The origin of the leak raises complex ethical questions for journalists. Leaked documents may have been cherry-picked or manipulated in order to mislead. Even if the source material is authentic, there is a concern that strategic “hack-and-dump” operations may give a foreign agency undue influence over public discourse.

[Dearlove told Sky News in December](#) that the FSB hacked his encrypted emails in the first half of 2020 when he was “very active” with a group on Brexit. “I was exercising my democratic rights as a citizen to be highly active politically,” he said.

The former MI6 chief told the programme that the FSB initially gave his emails to a journalist from The Grayzone, describing the reporter as “a Russian stooge”. The material had passed through the hands of Russia “so you couldn’t trust that the emails were exactly how they existed when I read and received them,” he said.

Computer Weekly and *Byline Times* have undertaken extensive analysis of the leaked emails, both to check for signs of manipulation and to corroborate their contents. Careful examination shows that the hackers’ claims about a “deep state” coup are clearly overblown. Instead, the emails reveal an informal and often amateurish lobbying campaign involving retirees from the intelligence services, the military and academia.

## **The Cambridge two**

At the centre of the Protonmail network is an unlikely duo: Richard Dearlove, a former head of the British Secret Intelligence Service (known as MI6), and Gwythian

Prins, a historian and former Nato adviser. In demeanour, the two men are opposites: Dearlove terse and imperious; Prins excitable and ingratiating.

When the pair appeared together on a panel at the National Conservatism conference, Dearlove delivered his speech in a dull monotone, while Prins launched into a rendition of *The Skeleton Dance* (“the knee-bone’s connected to the thigh-bone, the thigh-bone’s connected to the hip-bone”) to demonstrate the interconnected nature of the “woke agenda”.



Sir Richard Dearlove (left) and Gwythian Prins (right) speaking at the 2023 Nat Conservatism conference

But they share certain affinities. Both men are in their 70s. Both were educated and later worked at Cambridge University: Prins as a lecturer in history and politics; Dearlove as master of Pembroke College. Both are foreign policy hawks, with ties to bastions of neoconservatism like the Henry Jackson Society.

Both have roots in the West Country and enjoy countryside pursuits. Prins keeps his beloved horse, Crunchie, at his estate in Devon and is a “passionate fox hunting man”; Dearlove splits his time between Cambridge and Cornwall and is an “accomplished salmon fisherman”.

Perhaps most importantly, both men appear to feel a deep sense of alienation from the institutions that shaped them. Dearlove writes that two of his former MI6 colleagues now regard him as a “dangerous radical”; Prins says he was “unable to digest or be digested” by Cambridge. Prins cannot even find refuge in his Pall Mall

private members club, the Athenaeum, where he recently organised a protest against the “excessively woke” chairwoman who wants to relax the dress code.

Together, Dearlove and Prins coordinated a series of multi-pronged influence campaigns, combining public advocacy, private lobbying and covert operations. They sought to influence government on a wide range of issues – from Brexit to cyber security, climate change to Covid, satellites to nuclear power.

Their ideology is rooted in nostalgia for the moral clarity of the Cold War, with China replacing the Soviet Union as the biggest threat to the West. Every issue, foreign or domestic, is seen through a global geopolitical lens.

In briefings for MPs and ministers, they argued that Chinese company Huawei should be blocked from the UK's 5G network, that green energy policies were “economic self-harm” encouraged by China, that the government should invest in an alternative Covid vaccine based on the “lab leak” theory of the pandemic, and that any type of participation in EU defence policy would threaten the Five Eyes intelligence sharing alliance and Nato.

## **The email network**

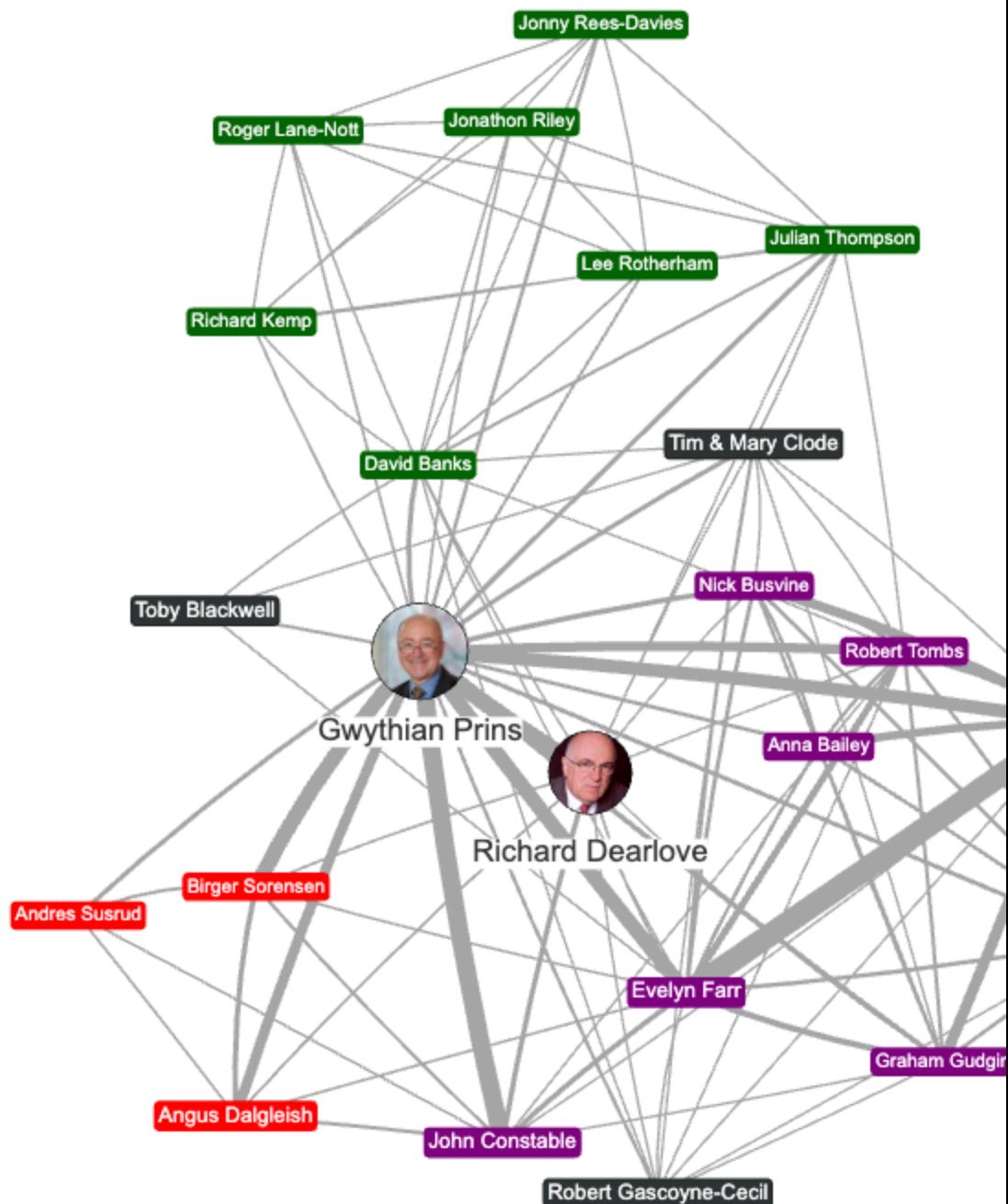
Computer Weekly and *Byline Times* have mapped the connections between people in the leaked dataset. It reveals three distinct clusters: Veterans for Britain (originally Veterans for Brexit), a pro-Brexit pressure group that included senior retired military officials; Briefings for Britain, a pro-Brexit website set up by two Cambridge academics; and a team of scientists developing an alternative Covid vaccine.

The leaked emails provide a rare insight into who was funding these campaigns. Julian “Toby” Blackwell, the 94-year-old former owner of the eponymous book retailer, emerges as the main donor behind Veterans for Britain. Email correspondence indicates that Blackwell paid £89,000 to a single staff member and agreed to contribute £20,000 towards Prins' living expenses. Prins reports that Blackwell donated over £1m to pro-Brexit campaigns in total.

The other main funders are Timothy and Mary Clode, a married couple based in Jersey. Emails indicate that the Clodes contributed tens of thousands of pounds to this network of campaign groups.

## Mapping the 'Sneaky strawhead' email network

Key clusters: **Veterans for Britain**, **Briefings for Britain**, **Covid research**



Width of line indicates number of emails between nodes (frequent senders only). [Full Chart](#): Sophie Hill



Like Blackwell, Timothy Clode worked in the publishing industry. He was managing director of Octopus Publishing Group for a decade before he resigned in 1986 and moved overseas. The following year, Octopus was sold to Reed International for over £500m. Clode is a major collector of British art, and there is a gallery at Gainsborough's House in Suffolk named after the couple.

Another key patron is Robert Gascoyne-Cecil, the 7th Marquess of Salisbury, and former Conservative MP and peer. He took a leave of absence from the House of Lords in 2001 in protest at new financial disclosure rules, then retired in 2017.

Salisbury provided some financial support, with emails indicating that he paid £5,000 for PR work by David Burnside, the former Ulster Unionist MP, and his lobbying firm New Century Media. He also hosted key meetings of the group at his property in Swan Walk, Chelsea, and recruited international allies, such as the US Ambassador and Australian former government ministers.

Timothy and Mary Clode declined to comment via a family member. Toby Blackwell, Lord Salisbury and Richard Dearlove did not respond to repeated requests for comment. Prins told Computer Weekly that “nothing which is the result of a proven FSB hack can be relied upon” and did not comment on the specific claims made in this piece. Dearlove previously acknowledged that his Protonmail account had been hacked in [an article](#) for *The Spectator*.

---

## Key figures

- **Richard Dearlove** (78) – ex-head of MI6.
  - **Gwythian Prins** (73) – historian and former NATO adviser.
  - **Robert Gascoyne-Cecil** (77) – Marquess of Salisbury, ex Tory MP and peer.
  - **Julian “Toby” Blackwell** (94) – former owner of Blackwell's publishing group.
  - **Timothy Clode** (76) – former publishing executive, Jersey resident, art collector.
-

Dearlove previously told Reuters that the emails captured a “legitimate lobbying exercise”, which was being distorted by the hackers. Fair enough, as far as it goes: Dearlove and Prins devoted much of their energy to drafting expert briefings and placing op-eds in newspapers, typical activities for any campaign group. But they were also willing to use the political “dark arts” to achieve their goals.

## **September 2018: Project C**

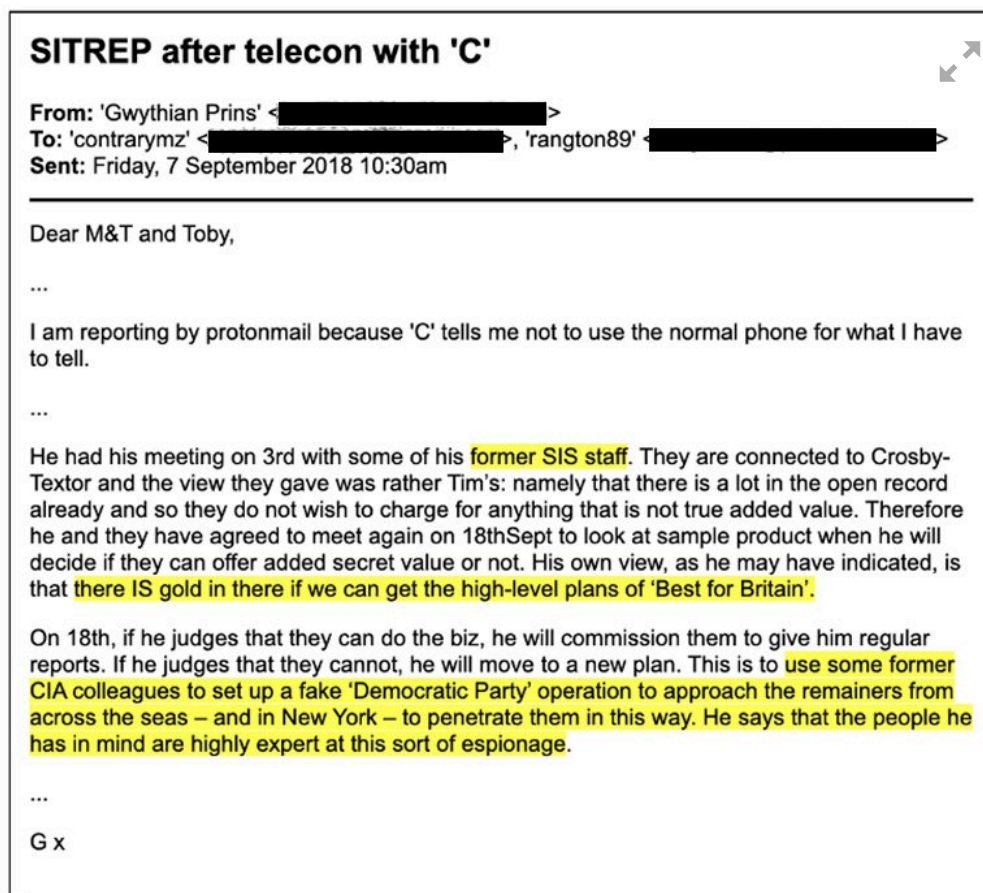
To accompany their public advocacy on Brexit, Dearlove and Prins planned a covert operation (codenamed Project C, after the nickname given to heads of MI6) to hire ex-spies to gather intelligence on pro-EU campaigners and civil servants, with Blackwell and Clode providing financial backing.

In an email from September 2018, Prins tells the donors that Dearlove recently met with “former SIS staff” and is awaiting “sample product” to see if they can “offer added secret value”. He says that Dearlove believes “there IS gold in there if we can get the high-level plans of ‘Best for Britain’,” referring to the pro-EU campaign group.

Prins says Dearlove also has an alternative plan to “use some former CIA colleagues to set up a fake ‘Democratic Party’ operation to approach the remainers from across the seas – and in New York – to penetrate them in this way”, noting that they are “highly expert at this sort of espionage”.

After further discussions, the group decided to target civil servants instead of campaigners, focusing in particular on Oliver Robbins, the chief Brexit negotiator under Theresa May, who was suspected of pro-EU tendencies. There is no evidence in the leaked emails that the group went through with these plans.





## 2018-2022: “The Mole”

Prins and Dearlove hoped to expose a Remain conspiracy inside the civil service using their “mole”, a fellow Brexit-supporter named Evelyn Farr. Farr is a historian and has published two books on the correspondence of Marie-Antoinette. She worked as a contractor in the civil service from 2016 to 2022, helping to project manage EU Exit legislation. Under her pseudonyms Caroline Bell and Ian Moone (anagram of “I am no one”), she wrote briefings giving an insider’s perspective on Brexit preparations. Some were published online, while others were delivered in secret to MPs and ministers.

But she did not confine herself to commentary on Brexit. In February 2022, after a meeting arranged by Prins, Farr wrote a briefing about the Online Safety Bill for the home secretary, Priti Patel, warning that it created a potential “back door” for hostile governments to access private communications in the UK, and citing concerns that “trans activists” and “BLM activists” could use the law “to ‘cancel’ people they disagree with”.

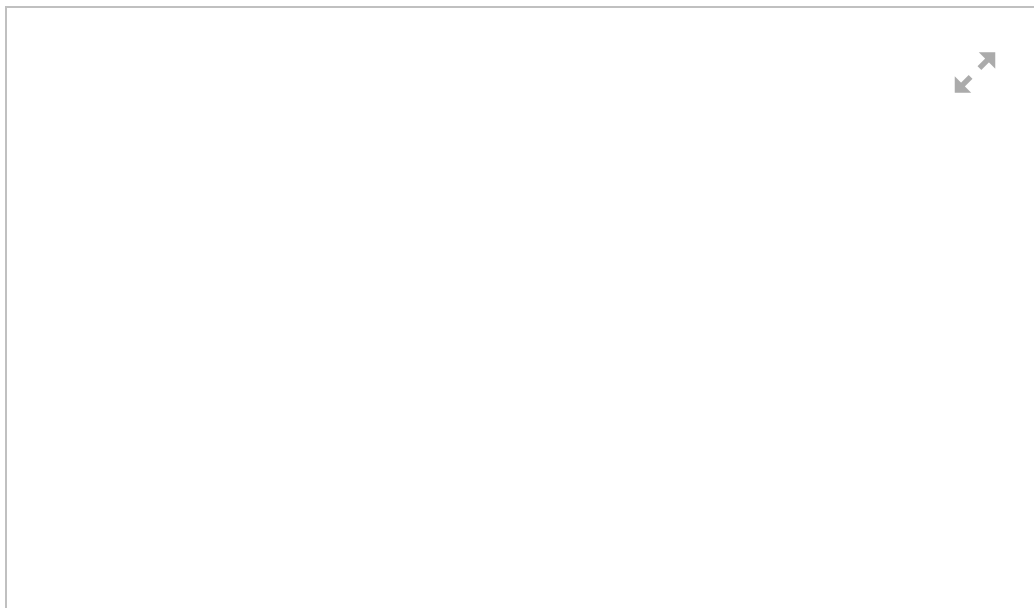
After the hack, Farr wrote a [blog post](#) confirming that she was the author behind the pseudonym Caroline Bell. She said the civil service opened an investigation into a “potential security breach”, which she believed was “a smokescreen to interrogate me about the briefings for ministers”. When contacted by Computer Weekly, Farr said she had no further comment beyond what she had written in the blog post.

## 2020-2022: The Covid Hunters

As [reported previously](#) by Computer Weekly and *Byline Times*, Dearlove and Prins planned a covert attack on the prestigious science journal, *Nature*. After the journal rejected a paper by the scientists Birger Sørensen and Angus Dalgleish that claimed Covid-19 originated in a lab leak, Dearlove and Prins began making baseless accusations that the editorial staff were “Chinese agents of influence”.

Emails reveal that Prins asked Michael Gove, then cabinet secretary, to put editorial staff at *Nature* under government surveillance. Dearlove contacted a former Foreign Office official with a similar request, urging “the powers that be” to have them “on a warrant”, because he expects them to “be in touch with the Chinese for instructions”.

There is no credible evidence to support the accusations made by Dearlove and Prins. Dearlove himself received a more plausible explanation of why the paper had been rejected when a publishing executive told him that it was “written as a stream of consciousness rather than as a scholarly/scientific paper”.



## The former 'C'

As head of MI6 during the 2003 invasion of Iraq, Dearlove played a key role in supplying the intelligence about supposed weapons of mass destruction to prime minister Tony Blair. When the Chilcot report was finally published in July 2016, it singled out Dearlove by name, stating that his “personal intervention, and its urgency, gave added weight to a report that had not been properly evaluated”.

The criticism clearly stung. Dearlove had spent a decade out of the spotlight as master of Pembroke College, Cambridge. But the Chilcot report and the Brexit vote seemed to mark a turning point. In the following years, Dearlove began making political interventions that would previously have been unthinkable for a former intelligence chief.

On the eve of the 2017 general election, he called Labour leader Jeremy Corbyn a “danger to the nation” who wouldn’t clear the security vetting at MI6. In 2018, he sent a letter to Conservative association chairs, accusing Theresa May of surrendering Britain’s national security with her Brexit deal and urging them to lobby their MPs to vote against it.

More recently, Dearlove spoke at the controversial National Conservatism conference and has been a regular guest on the right-wing broadcaster GB News, appearing five times since the channel’s inception.

Despite this, Dearlove retains the usual retirement perks of a former intelligence chief. He left his post at Cambridge to become chair of the board of trustees of the University of London. He sits on the board of companies in oil exploration, insurance and cyber security. As a director at Dallas-based Kosmos Energy, Dearlove has earned over \$2.6m in fees and stock awards since 2012. He even co-hosts a popular current affairs podcast.

While he rarely holds back when criticising others, Dearlove is more sanguine when assessing his own record. Two decades on from the invasion of Iraq, he was interviewed on a BBC podcast and asked whether the intelligence about weapons of mass destruction was fundamentally wrong. His response: “No, I don’t think it was.

This is a really complex issue, and I don't think people understand how complex it is."

## The last of the neocons?

Dearlove's sidekick and "co-conspirator" also underwent a dramatic political evolution throughout his career. Gwythian Prins – then known as "Gwyn" – began his career in the 1970s as a historian at Cambridge University researching the early colonial era of Western Zambia. Several years of fieldwork in Africa yielded a well-reviewed academic book and swashbuckling stories of encounters with guerrilla fighters.

Prins became a well-known advocate of nuclear disarmament, editing a 1984 book of essays called *Defended to death*, which argued that the North Atlantic Treaty Organisation (Nato) was "becoming a suicide pact".

Despite this trenchant critique, Prins was later recruited to join Nato as an adviser by his "old friend" Christopher Donnelly, a special advisor at Nato on central and eastern European affairs. He also worked at the Ministry of Defence's science and technology arm, the Defence Evaluation and Research Agency.

By the early 2000s, Prins was an established geopolitical hawk. An outspoken supporter of the invasion of Iraq, he argued that removing a tyrant was justification enough, regardless of whether weapons of mass destruction existed.

His academic background and prodigious capacity to write made him useful to politicians and military leaders seeking to influence defence policy. Prins regularly convened seminars and co-authored papers with figures like Lord Salisbury and Vice Admiral Jeremy Blackham.

His collaboration with Dearlove began in a similar vein. The two men crossed paths in the aftermath of the Brexit vote, galvanised by the perceived betrayal of Theresa May's withdrawal agreement. They made a good team, with Dearlove providing credibility and contacts, and Prins doing most of the legwork.

But, for them, the referendum was a Pyrrhic victory. They were experts in a movement that has "had enough of experts"; grand strategists in a party more

interested in culture wars than actual wars; a pair of neocons among the NatCons.

The hackers behind the “sneaky strawhead” leak claimed to have uncovered the machinations of the British deep state. But a careful analysis of the emails reveals something quite different: a network of elderly right-wing elites, marginalised by the realignment of the Conservative party, who struggled to translate their access to policymakers into influence.

The government has warned that Russian hacking operations may pose a threat to our democracy. In this case, the leaked material is more likely to embarrass than to destabilise. But it is an urgent reminder that our system of lobbying regulation is not fit for purpose.

Dearlove and Prins ran a years-long political influence campaign funded by wealthy private donors. They met with senior government ministers and sent regular briefings to Number 10. Without the “sneaky strawhead” leak, the scale of this activity would never have come to light. The public has a right to know who has the ear of government – and they should not have to rely on the operations of a foreign intelligence agency to find out.

---

## The Brexit conspiracy files

This story is part of an investigative series by Computer Weekly and *Byline Times*, examining the activities of a group of self-appointed lobbyists and hard Brexit supporters who attempted to influence government policy on science, technology, climate change and the environment post-Brexit. The secretive group were typical English good chaps, former Cambridge academics, doctors, members of the military, and highly placed civil servants. Led by a former head of MI6, Richard Dearlove, and former history professor Gwythian Prins, they had the ear of Number 10, the Cabinet Office and government ministers. They operated in secret using encrypted email and encrypted WhatsApp phone calls, until their activities were exposed by a Russian hacking group working for the FSB who gained access to Protonmail accounts

used by members of the group and published their emails on the internet. Computer Weekly and *Byline Times* have systematically analysed 22,002 leaked documents.



**ComputerWeekly.com**

---

### Read more coverage of the Brexit Conspiracy Files

- A [hacking operation by Russian-linked ColdRiver group](#) exposed former MI6 chief Richard Dearlove's contacts and email communications with government, military, intelligence and political officials.
- [MI6 chief's hacked emails attacked MI5](#) and betrayed British spy operations in China.
- [A conspiratorial group of extreme Brexit lobbyists mounted an extraordinary campaign](#) against one of the world's most prestigious science journals, *Nature*.

## ➤ Read more on Regulatory compliance and standard requirements

Tech specialist files legal claim after being refused security clearance for MI6 role

By: Bill Goodwin

Top 10 surveillance, journalism and encryption stories of 2024

By: Bill Goodwin

GCHQ to protect politicians and election candidates from

Top 10 investigations and national security stories of

## cyber attacks

By: Bill Goodwin

2023

By: Bill Goodwin

Latest TechTarget  
resources

CIO



SECURITY

NETWORKING

DATA CENTER

DATA MANAGEMENT

## Search CIO

**Project vs. program vs.  
portfolio management,  
explained**

Project, program and portfolio management are related, but they represent three distinct disciplines. Learn about the ...

**Capital One AI partnerships  
aim to build trust, grow  
talent**

Capital One's relationships with the National Science Foundation and several universities seek to improve AI's responsiveness and...



<a href="#">About Us</a>	<a href="#">Corporate Site</a>	<a href="#">Opinions</a>
<a href="#">Editorial Ethics Policy</a>	<a href="#">Contributors</a>	<a href="#">Quizzes</a>
<a href="#">Meet The Editors</a>	<a href="#">Reprints</a>	<a href="#">Photo Stories</a>
<a href="#">Contact Us</a>	<a href="#">Answers</a>	<a href="#">Tips</a>
<a href="#">Our Use of Cookies</a>	<a href="#">E-Products</a>	<a href="#">Tutorials</a>
<a href="#">Advertisers</a>	<a href="#">Events</a>	<a href="#">Videos</a>
<a href="#">Business Partners</a>	<a href="#">In Depth</a>	<a href="#">Computer Weekly Topics</a>
<a href="#">Media Kit</a>	<a href="#">Guides</a>	

©2025 TechTarget, Inc. d/b/a Informa TechTarget. All Rights Reserved.

[Privacy Policy](#)

[Cookie Preferences](#)

[Do Not Sell or Share My Personal Information](#)



This website is owned and operated by Informa TechTarget, part of a global network that informs, influences and connects the world's technology buyers and sellers. All copyright resides with them. Informa PLC's registered office is 5 Howick Place, London SW1P 1WG. Registered in England and Wales. TechTarget, Inc.'s registered office is 275 Grove St. Newton, MA 02466.